Sveučilište u Zagrebu
Fakultet političkih znanosti
Diplomski studij novinarstva

Ana-Maria Kezerić

Analiza prijetnji i rizika cyber sigurnosti Republike Hrvatske: ranjivost informacijske infrastrukture

DIPLOMSKI RAD

Zagreb, 2017.

Sveučilište u Zagrebu
Fakultet političkih znanosti
Diplomski studij novinarstva

Analiza prijetnji i rizika cyber sigurnosti Republike Hrvatske: ranjivost informacijske infrastrukture

DIPLOMSKI RAD

Mentorica: doc.dr.sc. Ružica Jakešević
Sumentor: prof.dr.sc. Dario Matika
Studentica: Ana-Maria Kezerić

Zagreb,
rujan 2017.

Izjavljujem da sam diplomski rad **„Analiza prijetnji i rizika cyber sigurnosti Republike Hrvatske: ranjivost informacijske infrastrukture“**, koji sam predala na ocjenu mentorici doc.dr.sc. Ružici Jakešević, napisala samostalno i da je u potpunosti riječ o mojem autorskom radu. Također, izjavljujem da dotični rad nije objavljen ni korišten u svrhe ispunjenja nastavnih obaveza na ovom ili nekom drugom učilištu, te da na temelju njega nisam stekla ECTS-bodove.

Nadalje, izjavljujem da sam u radu poštivala etička pravila znanstvenog i akademskog rada, a posebno članke 16-19. Etičkoga kodeksa Sveučilišta u Zagrebu.

Ana-Maria Kezerić

Mojoj obitelji.

Jer ste uvijek vjerovali u mene.

Veliko, ogromno, najveće hvala profesoru Dariu Matiki s Vojnog Učilišta, koji nije bio samo moj sumentor, *već nerijetko i psihijatar, prijatelj i podrška. Hvala, profesore, što ste mi otvorili „prozor“ u jedan sasvim novi svijet i na svim savjetima, predavanjima, znanju i pomoći koju ste mi pružili.*

SADRŽAJ:

POPIS ILUSTRACIJA

Tablice

Grafikoni

1. UVOD

Da nema nedodirljivih i da cyber prijetnje i u Hrvatsku ulaze na velika vrata, ukazuje hakerski napad na Ministarstvo vanjskih i europskih poslova (MVEP). Nasreću, hakeri se nisu domogli povjerljivih podataka, ali i sam njihov akt ozbiljna je ugroza nacionalne sigurnosti, osobito s obzirom na činjenicu da su probili sustav koji je umrežen s Uredom predsjednice i premijera (Latković, 2016). Nisu hakeri prvi puta u 2016. upali u MVEP, ali i druga ministarstva i državne i privatne tvrtke i organizacije. Na ranjivost sustava stručnjaci iz Centra informacijske sigurnosti (CIS) upozoravaju odavno, ali očito ne dovoljno glasno da bi ih se shvatilo ozbiljno. Cyber više nije tek svijet gamera i geekova, on sve više postaje prefiksom i za terorizam, kriminal, prijetnje, rat. CIS[1] je provale na hrvatske web poslužitelje pratio od 2011. i upozoravao vlasnike stranica na kompromitaciju i upade. Dvije godine kasnije odustali su jer „mnogi pružatelji usluga često nisu navedene prijetnje shvaćali ozbiljno, te su često sporo reagirali na upozorenja“ (CIS, 2013).

Kada se tome pribroji i očiti nedostatak društvene volje i svijesti o novim ugrozama, prvenstveno na državnoj razini (do 2015. nismo imali niti Nacionalnu strategiju kibernetičke sigurnosti, a novu Strategiju nacionalne sigurnosti dobili smo nakon punih 15 godina) ne čudi da običan, prosječni građanin nema ideju o cyber (ne)sigurnosti i mogućim oblicima zaštite. Prema posljednjem istraživanju Državnog zavoda za statistiku (DZS), o primjeni informacijskih i komunikacijskih tehnologija (IKT) u kućanstvu, glavni nalazi istraživanja ukazuju da je 77 posto hrvatskih kućanstva u 2016. godini imalo pristup internetu. Također, više od 50 posto građana prilikom izrade popisa stanovništva 2011. izjavilo je da se zna služiti internetom. Nadalje, kako pokazuju podaci DZS-a, ukupan podatkovni promet u četvrtom tromjesečju 2016. iznosio je 201 milijun gigabajta. U porastu je i trgovina putem interneta te korištenja usluge elektroničkih servisa kao što je e-vlada. Sukladno globalnom trendu, gotovo sve što je dosad bilo jedino opipljivo i materijalizirano u stvarnom svijetu, seli se u virtualnu zajednicu. To sa sobom nosi mnoštvo prednosti, ali i nedostataka, a jedan od njih zasigurno je ranjivost kritične informacijske infrastrukture i opasnost od cyber napada. U takvim okolnostima, i pitanje (nacionalne) sigurnosti djelomično fokus premješta na cyber, odnosno, kibernetičku sigurnost.

[1] Evidencija provala na hrvatske web stranice koju je Centar informacijske sigurnosti pratio do 2013. godine i dalje je dostupna na njihovim internetskim stranicama http://www.cis.hr/opcenito/evidencija-provala-na-hrvatske-web-stranice.html.

Cyber svijet je nešto što se mijenja na svakodnevnoj razini i čemu se potrebno prilagođavati jer se dotiče svake razine društva i države. Upravo zato, neophodno je kritički sagledavati postojeću informacijsku infrastrukturu i analizirati postojeće prijetnje i rizike koje donosi suvremeno, kibernetičko doba. Analiza prijetnji i rizika potrebna je kako bismo se s njima mogli adekvatno suočiti i predvidjeti teškoće koje bi nam se mogle naći na putu, a koje bi mogle imati i značajne posljedice za nacionalnu sigurnost. Stoga ovaj diplomski rad ima za cilj dati mali doprinos još uvijek neistraženoj temi u Republici Hrvatskoj, ali i potaknuti društvenu svijest o opasnostima koje nam kucaju na vrata.

Rad je podijeljen na pet poglavlja u kojima će biti definirani informacijska i cyber sigurnost te glavne prijetnje koje ih ugrožavaju, kritična (informacijska) infrastruktura te politika informacijske sigurnosti u Hrvatskoj. Kroz studiju slučaja i GAP analizu razine informacijske sigurnosti u tri zdravstvene ustanove i jednoj energetskoj, nastojat će se ukazati na glavne slabosti u postojećim sustavima i politikama informacijske sigurnosti, kako bi se takvi nedostaci u budućnosti mogli izbjeći ili barem prevenirati.

2. INFORMACIJSKA SIGURNOST

Kada je riječ o informacijskoj sigurnosti, ne postoji sustav, podatak ili informacija koji su u potpunosti sigurni. Stručnjaci se tako vole našaliti da „jedini informacijski sustav koji je zaista siguran je onaj koji je ugašen, isključen iz napajanja, zaključan u sefu od titana, zakopan u betonskom bunkeru, te okružen nervnim plinom i dobro plaćenim naoružanim čuvarima“ (Spafford, prema Hadjina, 2009: 7). Kako dalje zaključuje Spafford, niti se tad baš ne bi kladio na njega. U svakoj je šali pola istine, pa je tako i s navedenim citatom o informacijskoj sigurnosti koja danas, više nego ikad postaje referentna točka baš svake državne, privatne, profitne i neprofitne organizacije. Važne informacije o poslovanju kompanija, državnim tajnama i povjerljivim pitanjima više nisu pohranjeni samo u debelim, starim registratorima ili sefovima. One se danas nalaze u računalnom oblaku, na internoj mreži pojedine tvrtke, računalu zaposlenika. Sigurnost tih podataka ne ovisi samo o hardverskoj i softverskoj zaštiti, već uvelike i o sigurnosnoj kulturi i (znanju o) postupanju zaposlenika s tim, nerijetko osjetljivim podacima.

Stoga se informacijska sigurnost može definirati kao očuvanje povjerljivosti, integriteta - cjelovitosti i dostupnosti - raspoloživosti (Brnetić i dr, 2013: 6), a koje se prema Zakonu o informacijskoj sigurnosti (Hrvatski Sabor, 2007) „postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda“.

2.1. Informacijski sustav

„Svi objekti na kojima se u nekom obliku nalaze sve informacije korporacije naziva se informacijski sustav. Informacijski sustav (IS) se može definirati kao sveobuhvatnost tehnološke infrastrukture, organizacije, ljudi i postupaka za prikupljanje, obradu, generiranje, pohranu, prijenos, prikaz te distribuciju informacija kao i raspolaganje njima.“ (Nađ i Adelberger, 2016: 117).

Ključni je element u tom sustavu informacija koja prestaje biti podatak u trenutku kada u određenom kontekstu dobije značenje. Primjerice, podatak mogu biti nepovezani pojmovi i brojke poput *789, CERT, 2015*, koji su neobrađeni i za pojedinca nemaju nikakvo značenje. Kada se ti podaci interpretiraju, dobivaju značenje za nekog pojedinca, korporaciju i/li instituciju. Tako prethodno nepovezani i beznačajni podaci dobivaju smisao kada kažemo*: Prema podacima CERT-a, 2015. godine u Hrvatskoj je zabilježeno 789 cyber napada*.

Nađ i Adelberger (2016: 118) navode resurske podrške u okviru informacijskog sustava, a koji se mogu definirati kao resursi unutar kojih se nalaze informacije. Tu spadaju hardver, softver, mreže, osoblje, mjesta, osnovne usluge te organizacijsko okruženje. Hardver čine fizički elementi uređaja za obradu podataka, softver logički dijelovi, odnosno, operativni sustavi i aplikacije, mreže se sastoje od „komunikacijskih sklopova korištenih za međuvezu nekoliko fizički udaljenih kompjutera ili elemenata informacijskog sistema“ (Nađ i Alderberger, 2016: 118). Osoblje čine svi zaposlenici i ljudi koji djeluju u okviru informacijskog sustava, pod mjestima se podrazumijevaju lokacije za smještaj fizičkih elemenata, a usluge mogu biti komunikacijske, komunalne i tome slično. Na kraju, organizacijsko okruženje prema autorima predstavlja kompletan organizacijski okvir, koji se sastoji od zaposlenika, pravila i procedura.

2.2. Aspekti informacijske sigurnosti

Aspekti informacijske sigurnosti povezani su kroz sigurnosni trokut (engl. *CIA triad*) koji sačinjavaju povjerljivost, cjelovitost i raspoloživost. Kako navodi Juran (2012: 19), u novije vrijeme navedenim kategorijama pojedini stručnjaci pridružuju i aspekte dokazivosti, autentičnosti i neporecivosti.

2.2.1. Povjerljivost

Kada je riječ o prvom aspektu informacijske sigurnosti, povjerljivosti, on se odnosi na očuvanje, odnosno zaštitu tajnosti podataka i nemogućnost da neovlaštene osobe pristupe tim podacima. Prijetnje narušavanju povjerljivosti podataka različite su, a najčešće je riječ o hakiranju, maskiranju, neovlaštenoj korisničkoj aktivnosti, nezaštićenom preuzimanju datoteka, trojanskim konjima i slično (Juran, 2012: 18).

“Napadi povjerenja su pokušaji upada u računalo ili mrežu kako bi nadgledali aktivnosti ili izvukli informacije iz sistema ili podatke korisnika. Vaganje takvog napada ovisi o količini izvučenih informacija i količini truda. Kriminalac koji ukrade bankovnu karticu ili špijun koji ukrade dizajn nekog aviona radi napad povjerenja, ali posljedice financijske prijevare ili špijunaže su očito drukčije“ (Singer i Friedman, 2014: 70).

Metode očuvanja povjerljivosti podataka jesu korištenje kontrole pristupa i metoda enkripcije. Kod kontrole pristupa podataka poanta je u tome da se kroz principe fizičke ili

logičke sigurnosti[2] ograniči pristup podacima koji su označeni kao klasificirani ili tajni te da do njih mogu doći samo ovlaštene osobe, dok je drugima kroz fizičku ili logičku kontrolu, pristup tim podacima onemogućen.

2.2.2 Integritet (cjelovitost)

Brnetić i dr. (2013: 6) integritet definiraju kao „zaštitu postojanja, točnosti i kompletnosti informacije kao i procesnih metoda". Integritet ili cjelovitost kao aspekt sigurnosnog trokuta odnosi se na činjenicu da podaci/informacije moraju ostati u neizmijenjenom obliku, cjeloviti i točni. Drugim riječima, prilikom obrade podataka i informacija, oni ne smiju biti modificirani, odnosno promijenjeni bez da su za to *zeleno svijetlo* dale ovlaštene osobe.

2.2.3. Dostupnost (raspoloživost)

Da bi bio ispunjen uvjet dostupnosti, podaci i informacije ovlaštenim (autoriziranim) korisnicima moraju biti pravovremeno raspoloživi i moraju im moći pristupiti kada god za to postoji potreba. "Napadi dostupnosti su oni koji brane pristup mreži, bilo da ju nadvlada količinom posjeta ili zabrani pristup ili ga čak skine s mreže i čak fizički ugasi virtualne procese koji o njoj ovise" (Singer i Friedman, 2014: 70).

2.3. Informacijska vs. informatička sigurnost

Područja informacijske sigurnosti navedena u Zakonu o informacijskoj sigurnosti (Hrvatski Sabor, 2007) jesu sigurnosne provjere, sigurnost podataka, fizička sigurnost, sigurnost informacijskih sustava i sigurnost poslovne suradnje. Kao što je razvidno iz te podjele, informacijska sigurnost obuhvaća puno šire područje od informatičke/računalne sigurnosti koja uglavnom pokriva samo *tehničke* dijelove sigurnosti. Kako rezimira Vuković (2012: 23), „informatička sigurnost samo je jedan dio informacijske sigurnosti koji se bavi tehnološkom zaštitom (npr. antivirusi, vatrozidovi, kriptiranje i sl.). Međutim informatička sigurnost ne pokriva npr. upravljanje ljudima koji su često vrlo velik izvor rizika".

[2] Fizička se sigurnost odnosi na zaštitu opipljive imovine, a logička na zaštitu neopipljive imovine, odnosno informacija i znanja. U prvom je slučaju riječ o upravljanju ljudskim resursima i imovinom, a u drugom o upravljanju tijekom informacija (Košutić i Matika, 2009: 180).

2.4. Informacijska sigurnost vs. cyber sigurnost

Informacijska sigurnost definirana je na prethodnim stranicama. No, kakve ona veze ima s danas, tako popularnim, pojmom cyber (kibernetičke)[3] sigurnosti? Poanta je ustvari vrlo jednostavna – budući da je većina informacija danas u digitalnom obliku, informacijska i cyber sigurnost mogu se smatrati gotovo sinonimima. Definicija cyber sigurnosti navedena u nizozemskoj Strategiji cyber sigurnosti iz 2011., a na koju se poziva Košutić (2012: 24), navodi da cyber sigurnost znači biti slobodan od opasnosti ili štete uzrokovane prekidom, ometanjem ili padom informatičko-komunikacijskih tehnologija (engl. *ICT*) ili zlouporabom ICT-a. Kako dalje navode, šteta prouzročena cyber napadom može se sastojati od „ograničavanja dostupnosti i pouzdanosti ICT-a, kršenja povjerljivosti informacija pohranjenim u ICT-u ili oštećenja integriteta tih informacija“ (Dutch Ministry of Security and Justice, 2011, prema Košutić, 2012: 24). Dakle, u navedenoj definiciji cyber sigurnosti možemo zamijetiti sva tri aspekta informacijske sigurnosti, odnosno, sigurnosnu trijadu.

„Cyber sigurnost je 95 posto informacijske sigurnosti“ (Košutić, 2012: 26). Kao jedinu razliku između njih, Košutić (2012: 26) navodi činjenicu da informacijska sigurnost uključuje sigurnost informacija i po pitanju nedigitalnih medija (papira), odnosno, sigurnost informacija u tradicionalnom obliku. S druge strane, cyber sigurnost fokusira se isključivo na sigurnost informacija u digitalnom obliku. „U mnogim slučajevima, informacijska sigurnost i cyber sigurnost korite se kao sinonimi, iako se čini da je cyber sigurnost poželjniji termin u vladinim krugovima u SAD-u, dok se pojam informacijske sigurnosti češće koristi u bankama i zdravstvenim organizacijama. Poanta je ovdje u sljedećem – pojmovi cyber sigurnosti i informacijske sigurnosti međusobno su zamjenljivi. Možete ih koristiti oba i nećete promašiti smisao“ (Košutić, 2012: 26).

2.5. „Mitovi“ o cyber sigurnosti

U današnjem svijetu cyber sigurnost velik je i neizostavan dio informacijske sigurnosti i kao takva će biti sagledana i u nastavku ovog rada. Međutim, cyber sigurnost ne

[3] U nedostatku boljeg prijevoda, ali i uzimajući u obzir ustaljenost i korištenje pojmova *cyber* i *kibernetika* u hrvatskome jeziku, u ovome će se radu ta dva termina koristiti kao istoznačnice, premda etimološki to nisu. Međutim, potrebno je objasniti gdje u hrvatskome jeziku dolazi do nesuglasica kada je u pitanju prijevod engleske riječi *cyber*. Kako objašnjava Vuković (2012: 16), „za pojam cyber još ne postoji ni ustaljen odgovarajući prijevod na hrvatski jezik“ te se taj termin, kako je navedeno u pojmovniku NSA-e, odnosi na svijet koji nastaje pomoću računala, dok je kibernetika znanstvena disciplina.

„vrti“ se samo oko novih tehnologija i nije jednokratan proces, što su najčešći mitovi koji se vežu uz nju. Tehnologija je samo jedan element uspješne politike informacijske sigurnosti[4], ali uz bok njoj stoje i osobe i procesi, čiju važnost ne treba zanemariti (Klaić, 2010: 1).

Upravo zato, Košutić (2012) upozorava na šest prevladavajućih mitova kad je riječ o cyber sigurnosti, osobito u modernim organizacijama. Riječ je o sljedećim mitovima:

1. Sve se vrti oko IT-a[5]
2. Cyber sigurnost nije problem top menadžmenta – oni nemaju ništa s tim
3. Većina (budućih) ulaganja u cyber sigurnost bit će u tehnologiju
4. Nema povrata investicije u sigurnost
5. Cyber sigurnost je jednokratan projekt
6. Mit o dokumentaciji.

„Zamislite ovaj scenarij: nezadovoljni administrator sustava namjerno je onemogućio jezgru sustava i izbrisao vaše najvažnije baze podataka. Je li to IT problem? Ne, teško da može biti, prije je problem ljudskih potencijala“ (Košutić, 2012: 17). Na tom primjeru jasno je vidljivo da se u cyber sigurnosti ne vrti sve oko IT-a. Sistemskom administratoru teško se može uskratiti pristup važnim aplikacijama, programima i podacima, jer mu je posao da upravlja njima. Ne postoji tehnički sustav zaštite hardvera ili softvera koji može spriječiti nekog od zaposlenika da sa samo nekoliko klikova mišem uništi povjerljivost, integritet i/li dostupnost. To se djelomično može prevenirati samo pametnim odabirom zaposlenika, nadzorom nad njima i politikama koje bi trebao donositi i provoditi odjel ljudskih potencijala, a koji se ne tiču tehnološkog aspekta posla.

Drugi se mit odnosi na ulogu top menadžmenta, odnosno odgovornih osoba neke organizacije ili kompanije koji najčešće sliježu ramenima i prstom upiru na IT odjel kao jedini zadužen za cyber sigurnost. Međutim, upravo su oni ti koje se prve treba uvjeriti da je cyber sigurnost važan projekt te da je potrebno osigurati novac i resurse za njega te razvijati sigurnosnu kulturu unutar cijele kompanije, počevši od njih. Jer kako opisuje Košutić (2012: 18), „ako se rukovoditelji ne ponašaju u skladu sa sigurnosnim pravilima i primjerice, ostave

[4] Politika informacijske sigurnosti „predstavlja dokumente kojima se utvrđuju mjere i standardi informacijske sigurnosti koje je potrebno primijeniti u informacijskom prostoru za zaštitu povjerljivosti, cjelovitosti i raspoloživosti podataka te raspoloživosti i cjelovitosti informacijskih sustava u kojima se ti podaci obrađuju, pohranjuju ili prenose“ (Klaić, 2010: 2).

[5] IT je kratica za *information technology*, odnosno, informacijsku tehnologiju koja obuhvaća alate za obradu informacija računalnim putem – računala, mreže i sustave.

laptop s popisom važnih klijenata i detaljima o prodaji i korespondenciji, nezaštićen na aerodromu, svi ostali sigurnosni napori bit će uzaludni“.

Većina kompanija u današnjem svijetu, pa i u Hrvatskoj, tehnologiju ima na zavidnoj razini. Opremljeni su novim, naprednim računalima i programima, stoga mit o ulaganjima u tehnologiju pada u vodu. Međutim, ono što tvrtke najčešće nemaju, jesu pravila o tome kako na siguran način koristiti ta računala, ne dovodeći u pitanje ugrožavanje podataka i informacija pohranjenih na njima. Nije riječ samo o pravilima, riječ je i o sigurnosnim procedurama, potrebi da svaki zaposlenik zna kojim podacima smije pristupiti, a kojima ne, te da je jasno naznačeno tko je odgovoran za koji dio informacije i opreme. To se postiže samo edukacijom i razvojem sigurnosne kulture te nadograđivanjem politike informacijske sigurnosti. U protivnom, posjedovanje visoke tehnologije je kao novi, luksuzni BMW koji koristite jedino za dostavu pizze (Košutić, 2012: 19-20).

Investicija u sigurnost višestruko se vraća onog trenutka kad se u nju uloži. Činjenica je da sigurnost košta i da možda povrat investicije neće biti vidljiv u *zelenim novčanicama,* ali bolje je *spriječiti nego liječiti*. Drugim riječima, razni sigurnosni programi koje pojedina organizacija implementira u većini slučajeva sačuvat će ih od sigurnosnih incidenata čije bi rješavanje i eliminaciju, da do toga dođe, platili puno više, ne samo novcem, već i gubitkom povjerenja partnera i reputacije.

Peti mit odnosi se na cyber sigurnost kao jednokratan projekt. Pojedine organizacije i laici misle kako je dovoljno jednom kupiti, primjerice, antivirusni program i sigurni su zauvijek. U takvo nešto teško je povjerovati jer se tehnologija razvija na dnevnoj bazi, a korak uz razvoj antivirusnih programa idu i oni koji razvijaju nove, još moćnije i razornije zlonamjerne programe. „Nadopuna (cyber) procedura i politika, ali i softvera, opreme i ugovora, posao je koji nikad ne završava“ (Košutić, 2012: 21).

Posljednji, ali ne i manje važan jest mit o dokumentaciji koji se odnosi na različite pisane politike i procedure koje same po sebi ne jamče sigurnost. Zaposlenici neke kompanije ili organizacije uglavnom neće sami po sebi prihvatiti takav dokument i sutradan ujutro doći na posao i slijediti sve sigurnosne procedure jer tako piše u novom pravilniku. Nisu potrebni samo dokumenti, već i vrijeme i trud da bi se neka loša navika promijenila, a dobra usvojila. Od te činjenice nije izuzeto niti pitanje sigurnosti i sigurnosne kulture.

3. PRIJETNJE INFORMACIJSKOJ SIGURNOSTI

Različiti autori različito definiraju prijetnje informacijskoj i cyber sigurnosti. Tako primjerice Košutić (2012: 12) prijetnje svrstava u prirodne katastrofe, vanjske maliciozne napade, interne napade te kvarove i nenamjerne ljudske greške. Na sličan način razvrstava ih i Hadjina (2009: 11) koji tvrdi da u uvjetima računalnih/informacijskih sustava postoje četiri opće vrste prijetnji: prirodne prijetnje, nenamjerne prijetnje (nesreće), namjerni aktivni ljudski napadi te namjerni pasivni ljudski napadi.

3.1. Razlika između rizika, prijetnje i ranjivosti

Prije sagledavanja kataloga prijetnji potrebno je precizirati razliku između rizika, prijetnje i ranjivosti. Ta tri pojma definirana su i u HRN ISO/IEC 27001:2005 te HRN ISO/IEC 17799:2005 normama, a citira ih Klaić (2010: 2): „Rizik predstavlja kombinaciju vjerojatnosti nekog događaja i njegovih posljedica (utjecaja). Prijetnja je potencijalni uzrok neželjenog incidenta koji može naštetiti sustavu ili organizaciji, a ranjivost je slabost nekog resursa ili skupine resursa koju može iskoristiti prijetnja".

Dakle, rizik je uvijek prisutan, a prijetnja se realizira ako iskoristi slabost, odnosno ranjivost nekog sustava te ona može prouzročiti štetu i izazvati pogubne učinke za neki sustav ili organizaciju.

3.2. Mapiranje kibernetskih prijetnji

Istraživački tim koji je nastojao mapirati prijetnje cyber sigurnosti Europske unije u studiji *Cyber sigurnost u Europskoj uniji i šire: istraživanje prijetnji i odgovora politika*[6], koju je naručio Europski parlament, navodi da ne postoji standardna ili univerzalno prihvaćena definicija cyber sigurnosti već da se prijetnje mogu ogledati kroz aktere, alate i tipove prijetnji te potencijalne mete.

Akteri prijetnji mogu biti države, kriminalci motivirani profitom, haktivisti i ekstremisti. Kao alate prijetnji navode *malware* i njegove varijante, kao što su bankarski (Trojan*), ransomware, point-of-sale malware, botnet* i programe za iskorištavanje (*exploits*).

[6] Originalni naziv studije iz 2015. godine, na engleskom je jeziku *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses*. Njezini su autori Nicole van der Meulen, Eun A Jo i Stefan Soesanto iz privatne istraživačke organizacije RAND.

Tipovi prijetnji jesu neovlašteni pristup, uništenje, objavljivanje informacija (kompromitiranje), mijenjanje informacije, uskraćivanje usluge. Mete mogu biti građani, vlade i organizacije. (Meulen i dr, 2015: 13).

3.3. Kategorije malicioznih napada

Vuković (2012: 17) maliciozne kibernetske aktivnosti dijeli na kibernetski kriminal, kibernetsku špijunažu, kibernetski terorizam i kibernetsko ratovanje. Toj se podjeli može dodati i u novije vrijeme, osobito raširen oblik hibridnog rata.

S obzirom na cilj, napadi mogu biti usmjereni na podatke ili nadzorne sustave (Vuković, 2012: 17). Kada je napad usmjeren na podatke, njegov je cilj da putem različitih alata (primjerice, DDoS napad)[7] ukrade ili uništi podatke te tako sabotira pojedinca, tvrtku ili instituciju, odnosno njihovu informacijsku imovinu. Druga vrsta napada jesu oni usmjereni na nadzorne sustave, a čiji je cilj penetracija u postrojenja koja su označena kao kritična infrastruktura i koji su neophodni za normalno funkcioniranje društva i života (primjerice elektroenergetski ili komunikacijski sustav).

Granice između pojedinih oblika malicioznih aktivnosti ponekad su jako tanke i isprepliću se. Vuković (2012: 18) u svom radu navodi dobar primjer Lecha J. Janczewskog i Andrewa M. Colarika koji cyber napade uspoređuju s provalom u bolničku bazu podataka. Kako navode, ako netko provali u tu bazu i prepiše lijek pacijentu koji je na njega alergičan, on će umrijeti. Riječ je o kibernetskom ubojstvu, odnosno, kaznenom djelu učinjenom pomoću računalne tehnologije, a koje se može protumačiti kao oblik kibernetskog kriminala. Ako isti taj napadač nakon takvog čina javnosti obznani da je to tek početak i da je u ostvarenju svojih ciljeva spreman počiniti još takvih i sličnih (ne)djela, tada je riječ o kibernetskom terorizmu. Pritom će kibernetski terorist vrlo vjerojatno pokušati ucijeniti primjerice, vlast neke države, iznoseći uvjete pod kojima će prestati sa svojim kriminalnim djelovanjem. Ako je cyber kriminalac/terorist i agent strane protivničkih struktura (primjerice suprotstavljene zemlje u ratu, strane obavještajne agencije i slično), tada je riječ o kibernetskom ratovanju.

[7] DDoS (*distributed denial of service)* je napad koji nastoji preopteretiti računalnu mrežu tako da se s više tisuća računala odjednom pokušava povezati na istu mrežu, kako bi se otežao ili onemogućio pristup određenoj računalnoj mreži i/li stranici.

3.3.1. Kibernetski kriminal

Kao što je već navedeno, riječ je o vrsti kriminala izvedenoj pomoću računalne tehnologije. Ta vrsta kriminala „obuhvaća prijevare na polju internetskog bankarstva i prijevare na Internetu s kreditnim karticama, a procjenjuje se kako je s godišnjom stopom rasta od oko 40 posto i s trenutnom zaradom od oko 100 milijardi dolara riječ o najbrže rastućem sektoru globalnog organiziranog kriminala“ (Vuković, 2012: 20).

U istraživanju koje je proveo Savić (2015) na Policijskoj akademiji, većina računalni kriminal vidi kao priličnu prijetnju nacionalnoj sigurnosti (njih 38 posto), dok nešto manji postotak polaznika Akademije prepoznaje opasnost kibernetskog kriminala povezanog s organiziranim kriminalom.

Pretpostavka je da će u budućnosti cyber kriminal još više rasti, kao i drugi pojavni oblici cyber (ne)djela zbog njihovih očitih prednosti. Prvenstveno, da bi *odradili* neki cyber napad, *srušili* internetsku stranicu NATO-a ili neke medijske kuće ili pak jednim klikom aktivirali bombu, možete se nalaziti na sasvim drugom dijelu svijeta, tisućama kilometara udaljeni od vaše mete.

Također, vrlo je vjerojatno da takvo što neće učiniti neuki i informatički nepismen pojedinac i da napad, dakako, neće izvesti sa svoje IP adrese i riskirati da mu naoružani specijalci upadnu u stan već će se, zahvaljujući svojim znanjima i vještinama, pobrinuti da mu se ne uđe u trag. Te vještine vrlo vjerojatno neće naučiti na kolegijima koje pohađa na faksu, ali nažalost ili nasreću, *Google* danas zna sve. Zahvaljujući informacijama kojima Internet (a osobito *dark web*) obiluje, vjerojatnije je da će potrebna znanja steći na raznim interaktivnim forumima i internetskim vodičima kojih ne nedostaje. Ili, kako to duhovito opisuje Glenny (2014: 14-15), „skupine staromodnoga organiziranog kriminala, privezane uz tehnologiju i sredstva dvadesetog stoljeća, trebaju svladati dvije zastrašujuće prepreke ne bi li u odabranom zanimanju požnjele uspjeh. Policija im je primarni poslovni rizik“. Kao drugi problem, navodi prijetnju koju im predstavlja konkurencija, odnosno drugi „loši momci i djevojke“ koji imaju iste ciljeve kao oni, a savezništvo među kriminalnim bandama uglavnom je put prema neuspjehu. Novi, „moderni“ pojavni oblici (cyber) kriminalaca 21. stoljeća takvih problema nemaju ili se barem s njima suočavaju u puno manjoj mjeri, a na ruku im ide i neusklađenost zakonske regulative po pitanju cyber zločina.

3.3.2. Kibernetska špijunaža

„Cyber špijunaža je akt ili praksa dobivanja tajne bez odobrenja nosioca informacija (osobnih, osjetljivih, vlasničkih ili tajnog karaktera), od pojedinaca, konkurenata, rivala, grupa, vlade i neprijatelja za osobnu, ekonomsku, političku ili vojnu prednost koristeći nelegalne metode na internetu, mrežama ili pojedinačnim računalima.. Za izvođenje cyber špijunaže uglavnom se koriste špijunski programi (*RAT, Keylogger*...), trojanski konji (specijalni trojanci napravljeni da špijuniraju korisnika), virusi... (Ugren, 2012: 11)“.

Kibernetska špijunaža može biti i jedan od elemenata kibernetskog i/li informacijskog rata. Uglavnom se najviše poistovjećuje s industrijskom špijunažom, ali nije rijetka niti na razini država ili od strane obavještajnih agencija neke zemlje. Kod kibernetske špijunaže važno je napomenuti da je računalo ponekad samo alat, odnosno, da je moguće da se izvede kroz napad na informatičku strukturu, odnosno, hakiranjem i krađom podataka, ali često može biti i rezultat socijalnog inženjeringa ili nepažnje zaposlenika.

3.3.3. Kibernetski terorizam

„Kibernetski terorizam označava promišljene, političke motivirane napade izvršene od strane nacionalnih skupina ili prikrivenih čimbenika, odnosno pojedinaca, usmjerene protiv informacijskih ili računalnih sustava, računalnih programa, te podataka, a koji rezultiraju nasiljem nad neborbenim metama“ (Vuković, 2012: 18-19).

Danas se kibernetika u smislu terorizma uglavnom još uvijek povezuje s korištenjem nove tehnologije od strane terorističkih skupina, osobito tzv. Islamske države Iraka i Levanta (ISIL). Proučavatelje cyber sigurnosti, ali i laike, prilično zabrinjava trend prisutnosti terorista na Internetu, a osobito društvenim mrežama preko kojih regrutiraju sljedbenike, ali i koordiniraju i dogovaraju napade. Ipak, neminovno je da će se cyber teroristi u narednim godinama obučiti i za sofisticirane napade informacijskom tehnologijom koja bi mogla rezultirati konkretnim ljudskim žrtvama. Upravo se kombiniranje kibernetskog terorizma s fizičkim teroristima pokazalo kao najučinkovitije. Primjerice, „onemogućavanjem komunikacijskog sustava hitnih službi tijekom fizičkog terorističkog napada, povećao bi se učinak fizičkog napada“ (Vuković, 2012: 18-19).

3.3.4. Kibernetski rat

„Kibernetski rat (engl. *Cyberwar* ili *Cyberwarfare*) prema enciklopediji Britannica je rat koji se vodi pomoću računala i mreža koje ih povezuju. Poduzet je od strane država ili drugih od njihove strane angažiranih subjekata protiv drugih država“ (Vuković, 2012: 19).

Ovakav oblik ratovanja zapravo je simbioza svih oblika i alata malicioznih aktivnosti i očituje se u kontinuiranim i učestalim napadima u ratu između dvaju država. Često se poistovjećuje s informacijskim ratom kojim se želi postići informacijska prednost nad protivnikom. To se postiže krađom protivničkih informacija te njihovom izmjenom. Danas se uglavnom govori o hibridnom obliku kibernetskog ratovanja, odnosno, hibridnom ratu koji bi se mogao opisati kao sprega kibernetskog i informacijskog ratovanja.

Različiti autori različitih su mišljenja o početku i uopće o postojanju kibernetskog rata. Clarke i Knake (2010, prema Kovačević, 2014: 92-3) kao početak cyber rata navode napad Izraela na sirijska nuklearna postrojenja Deir ez-Zor 2007. Izraelci su tom prilikom pomoću kontrole računalnog programa za radarski sustav onemogućili radarima da vide izraelske zrakoplove te su izveli zračni napad. Steinnon (2010, prema Kovačević, 2014: 93) kao početak kibernetskog rata navodi DDoS napad (*distributed denial of service*) na računalne sustave gruzijskog predsjednika i vladinih institucija. Kao krivce za taj napad Gruzijci vide Ruse. Treći događaj koji se spominje kao početak cyber rata jest napad visoko sofisticiranim crvom Stuxnet 2009. godine. Iako nikad nije dokazano, sumnja se da su Izraelci uz pomoć Amerikanaca poremetili rad iranskih nuklearnih postrojenja ubacivanjem virusa u infrastrukturni sustav.

3.3.5. Hibridni rat

Hibridni rat novi je model kompleksne otvorene uključenosti vojne, ekonomske i obavještajne sile kako bi se postigli određeni politički, gospodarski i ostali ciljevi. Kako navodi Bond (2007: 3-4) država koristi svoje vojne aktivnosti, resurse, programe i aplikacije kako bi maksimizirali nenasilne, političke i ekonomske faktore. Oni su prisiljeni pod takvim pritiskom reformirati vlastite trendove te se stvaraju nestabilni uvjeti te imaju karakter država pred urušavanjem. U takvom ratu ne preza se od korištenja punog spektra vojnog obavještajnog djelovanja, nekonvencionalnog oružja, naoružavanju određenih skupina, snaga za potporu i opremu za uključivanje, ako opozicija, regularne jedinice, teroristi i plaćenici ili drugi postanu direktna prijetnja tim neprijateljskim aktivnostima.

Hibridna je prijetnja fenomen koji proizlazi iz konvergencije i međupovezanosti različitih elemenata koji zajedno tvore još složeniju i višedimenzionalnu prijetnju. Često je korištena s referencama na hibridni rat kako bi se opisali složeni izazovi kao što su etnički sukobi, terorizam, migracija i slabost institucija. Kao ranjive sektore Dukić (2016: 34) označava energetski sektor, svemirsku infrastrukturu, pomorsku sigurnost, javno zdravstvo, zračni, pomorski, željeznički promet, komunikacije i financijske sustave. Zbog toga je Europska unija posebno ranjiva te se njezina suradnja s NATO-om povećala. Na nedavnom summitu u Varšavi, NATO je cyber prostor označio kao novo područje svojih operacija i akcija.[8] S EU je potpisao i Zajedničku deklaraciju koja se odnosi na suradnju u suprotstavljanju hibridnim prijetnjama. Ključna je odrednica da napadači na zajednički „teritorij" koriste internet kao oružje.

3.4. Cyber incidenti u Hrvatskoj i svijetu

Cyber kriminal svjetske tvrtke godišnje košta oko dva trilijuna dolara. Najveći dio napada odnosi se na svijet industrije te je pogođeno 21,5 posto poduzeća (Passeri, 2017). Na drugom mjestu je svijet financija s 15,1 posto. Ono na što upozoravaju informatički stručnjaci je da su sve više ugroženi i korisnici društvenih mreža. Maliciozni kodovi širili su se tako Facebookom i u studenom 2016. u Hrvatskoj. O tome je izvijestio i CERT kao i njegova stranica antibot.hr.

3.4.1. Svijet

a) Stuxnet

Maliciozni program, crv Stuxnet, otkriven je 2010. u postrojenju iranske tvornice za obogaćivanje urana. Bio je projektiran posebno za operativni sistem Windows i morao je zaraziti Siemensove industrijske kontrole. On je jedini to i uspio, a rezultat je bio devastirajući. Crv je uspio uništiti Siemensove centrifuge u nuklearnoj elektrani. To je napravio tako što im je zarazio program i promijenio brojeve okretaja. Dodatno je zastrašujuće što je crv to uspio sakriti od samih kontrolora. To je jedini takav maliciozni program za kojeg se pouzdano zna da je napravio štetu. Iako tvorac nikad nije otkriven, sumnja se da su ga izradili stručnjaci iz Izraela i SAD-a.

[8] NATO (2016) Warshaw Summit Communiqué. www.nato.int/cps/en/natohq/official_texts_133169.htm. Pristupljeno 9. veljače 2017.

b) Napad na Spamhaus

Spamhaus je jedan od najvećih svjetskih anti-spam servisa. Blokiraju velik broj neželjenih mailova u svim zemljama svijeta što se nije svidjelo Nizozemcima. Naime, njihov provider *Cyberbunker* otkrio je kako su njegovi mailovi dospjeli na Spamhausovu crnu listu. Zbog osvete su lansirali najveći DDoS napad u povijesti interneta. Promet prema Spamhausu narastao je na 300 gigabajta u sekundi što je usporilo sve velike internetske veze u Europi. Šef *Cyberbunkera*, Sven Kamphuis zbog toga je uhićen u Španjolskoj gdje trenutno čeka suđenje.

c) Ransomware WannaCry

Sredinom svibnja ove godine računalima diljem svijeta raširio se novi model *malwarea*, odnosno, *ransomware* nazvan *WannaCry*. Iskoristio je propuste u starijim verzijama Windowsa, kao i u novijim, koje nisu imale posljednje sigurnosne zakrpe. Ljudi bi ga uglavnom dobili kao datoteku u e-mailu ili kao URL vezu u poruci na društvenim mrežama. Zarazio je više od 200 tisuća računala u 150 zemalja.

WannaCry je iskorištavao ranjivi protokol imena *Eternalblue*. Tvorci WannaCry-a iskoristili su i špijunski alat *Doublepulsar* kojeg inače koristi američka agencija NSA (*National Security Agency*). Pomoću takvog pristupa ubacili bi malware u sistem i instalirali ga. On bi potom zaključavao računalo. Za otključavanje i potrebnu šifru tražio je uplatu određene svote novca u virtualnoj valuti Bitcoin. Prolaskom vremena ta bi se cifra konstantno povećavala, a istekom krajnjeg vremena obrisali bi se svi podaci sa zaraženog računala (CERT-EU, 2017).

Iako je zakrpa za tu ranjivost bila dostupna od ožujka 2017., brojna neažurirana računala stradala su prilikom ove vrste napada. Među prvima tako su stradali američka dostavna kompanija FedEx, španjolska telekomunikacijska kompanija Telefonica i najmanje 40 bolnica u Velikoj Britaniji. Njihov problem bio je stari operativni sustav Windows XP koji se prestao nadograđivati još 2014. godine. Nakon što je *WannaCry* poharao više od stotinu zemalja svijeta, Microsoft je odlučio izraditi zakrpu i za Windows XP.

Nacionalni CERT Hrvatske također je izdao upozorenje za novu vrstu *ransomwarea*. Napomenuli su kako ne preporučuju plaćanje otkupnine te da bi zaraženo računalo trebalo izdvojiti iz mreže. Osim toga, savjetovali su ljude da pokrenu backup podataka te ažuriraju svoje sustave i antivirusne programe. Zbog WannaCry-a problema su imali i u Ministarstvu

unutarnjih poslova Republike Hrvatske, gdje virus nije uspio srušiti sustav, ali ga je usporio, što je uzrokovalo smetnje u radu.

3.4.2. Hrvatska

U našoj zemlji, prema najnovijim dostupnim podacima, prijavljena su i obrađena 642 računalna incidenta, među kojima prednjače *web defacement (*kompromitirano web sjedište s izmijenjenom početnom web stranicom), *phishing*[9] *URL* i *malware* URL. (CERT, 2016). U phishing porukama napadači su se lažno predstavljali kao Google-ov tim, a zabilježeno je i nekoliko DDoS napada.

a) Ransomware

Maliciozni software koji ljudima zaključa računala i ne da im šifru dok ne uplate novac stvarao je Hrvatima najviše problema. Prema istraživanju Kaspersky Laba (2016), Hrvati su tu bili na drugom mjestu u svijetu, odmah iza Japana. Prema njihovu istraživanju napadnuto je 3,7 posto svih korisnika Kaspersky antivirusnih programa u Hrvatskoj. Taj problem, kao glavni, proglasio je i servis Antibot.hr (2016)[10].

b) SOA

Nepoznati hakeri domogli su se 400 gigabajta mailova talijanske kompanije Hacking Team koja prodaje softver za prisluškivanje komunikacija. Među njima bila je i njihova korespondencija sa Sigurnosno obavještajnom agencijom – SOA-om. To je objavljeno na Wikileaksu (2015) i ondje stoji kako je naša obavještajna služba željela kupiti softvere za nadgledanje Skype-a, Vibera i WhatsAppa. Osim toga, objavljeni su razgovori Talijana i još nekoliko hrvatskih tvrtki, piše CERT u svom izvješću.

c) Napad na internet bankarstvo

Nepoznati hakeri ubacivali su maliciozan softver i Trojance na računala Hrvata tijekom 2014. i pokušali su se domoći podataka pomoću kojih su ljudi pristupali internet bankarstvu. Probali

[9] *Phishing* je vrsta socijalnog inženjeringa u kojoj se zlonamjerni korisnici nastoje na prijevaru domoći povjerljivih podataka kako bi ih zloupotrijebili, najčešće sa svrhom ostvarivanja financijske koristi. To čine tako što šalju lažne poruke i linkove u e-mailu koje nalikuju, primjerice, na internetske stranice banaka. Ne znajući da je riječ o prijevari, korisnik upisuje ime i prezime, OIB, broj računa i slično, a ti su podaci automatski dostupni prevarantima.

[10] Riječ je o servisu CARNET-a i Nacionalnog CERT-a koji je pokrenut sa svrhom pomaganja internetskim korisnicima u čišćenju računala od zlonamjernih programa i prevenciji zaraze. (Antibot.hr, 2017.)

su se domoći gotovo 12 milijuna kuna. Sve to istražuje policija. Hrvatska narodna banka (HNB) izvijestila je da su se hakeri ukrali 1,8 milijuna kuna (Ivezić, 2014).

4. KRITIČNA INFRASTRUKTURA

Hakiranje internetskih stranica, krađa podataka s bankovnih kartica, upadi u računala i e-mailove, virusi, crvi... U svijetu u kojem živimo, sve su to postali uobičajeni pojmovi s kojima se ljudi na dnevnoj bazi više ili manje susreću, ali ih uglavnom više ne začuđuju, jer su svjesni da i oni sami prije ili kasnije mogu postati žrtva nekog takvog napada. Međutim, pomisao na mogućnost raspada elektroenergetskog sustava, hakiranja aviona i pacemakera ili pak potpunog prekida komunikacija, nije toliko prisutna u mainstreamu i javnom diskursu. Takve se stvari većini ljudi još uvijek čine kao rezervirane za filmove ili znanstvenu fantastiku, dok su sigurnosni stručnjaci i vlade većine zemalja ozbiljno zabrinuti zbog realne mogućnosti takvih scenarija.

Posljedice (cyber) napada na kritičnu infrastrukturu, odnosno, SCADA sustave na kojima počiva velik broj postrojenja koja su dio te infrastrukture, Blunden (2010: 11, prema Kovačević, 2014: 97) s pravom opisuje kao cyber Katrinu, navodeći da bi „uspješan cyber-napad na mreže koje upravljaju vitalnom infrastrukturom cijelu Ameriku pretvorio u jedan veliki Saint Louis poslije uragana Katrina“.

Hrvati su samo mali djelić takve situacije mogli osjetiti kada je krajem rujna 2015. došlo do pada T-com-a te prekida fiksne i mobilne telefonije te interneta. „Kao posljedica tog događaja došlo je do značajnih negativnih učinaka poput potpune nedostupnosti Nacionalne službe za hitne slučajeve 112 i pada sustava za interne POS, ali i međunarodne (SWIFT) transakcije. Osim toga, do 13 sati bili su blokirani ili su radili s poteškoćama Zagrebačka burza, Hrvatski zavod za zdravstveno osiguranje, Hrvatska pošta, Porezna uprava i većina drugih službi koje se u svom poslovanju oslanjaju na telekomunikacijsku uvezanost“ (Brzica, 2015: 33). Iako nije bila riječ o hakiranju, već kvaru sustava, taj je primjer ukazao na slabosti kritične (informacijske) infrastrukture te nužnosti bolje zaštite.

Republika Hrvatska Zakon o kritičnim infrastrukturama donijela je 26. travnja 2013. godine. Kao nacionalnu kritičnu infrastrukturu, spomenuti Zakon prepoznaje „sustave, mreže i objekte od nacionalne važnosti čiji prekid djelovanja ili prekid isporuke roba ili usluga može imati ozbiljne posljedice na nacionalnu sigurnost, zdravlje i živote ljudi, imovinu i okoliš, sigurnost i ekonomsku stabilnost i neprekidno funkcioniranje vlasti“ (Hrvatski Sabor, 2013). Kao sektori nacionalnih kritičnih infrastruktura u Zakonu o kritičnim infrastrukturama

navedeni su energetika, komunikacijska i informacijska tehnologija (elektroničke komunikacije, prijenos podataka, informacijski sustavi, pružanje audio i audiovizualnih medijskih usluga), promet, zdravstvo, vodno gospodarstvo, hrana, financije, proizvodnja, skladištenje i prijevoz opasnih tvari, javne službe, nacionalni spomenici i vrijednosti.

Slaveski i Popovska (2015: 35-36) upozoravaju na nedostatke SCADA sustava. Osim problema kao što su isti operativni sustav, nedostatak okruženja u kojem bi cyber sigurnost države mogla biti testirana, lokalnu upravu i nepostojanje nadzora, navode i ljudski faktor, s naglaskom na moguću pogrešku zaposlenika koje je puno lakše napasti nego sam sustav, a zbog čijih grešaka može proizaći i napad na sustav. „Vlasnici ovih sustava vjeruju da će biti zaštićeni samim time ako su nepoznati javnosti i da nitko neće hakirati njihov sustav. Misle da su neprobojni jer je njihov program dizajniran specijalno za njih (...) Većina tih sustava koristi iste protokole koji su razvijeni/napisani u istom programskom jeziku poput svih ostalih programa koji se danas nalaze na tržištu, a u kojima je relativno jednostavno naići na propuste“ (Slaveski i Popovska, 2015: 35-36).

4.1. Kritična informacijska infrastruktura

Informacijsku infrastrukturu možemo definirati kao „kombinaciju računalnih i komunikacijskih sustava koji služe kao temeljna infrastruktura javnim tijelima, industriji i gospodarstvu. Kritične infrastrukture kao što su prijevoz i distribucija električne energije nužno ovise o telekomunikacijskoj, javnoj telefonskoj mreži, internetu, zemaljskim i satelitskim bežičnim mrežama i povezanim računalnim resursima za upravljanje informacijama, komunikacijom i kontrolom“ (Brnetić i dr, 2013: 6).

Upravo ta međuovisnost ono je što sustave, odnosno, infrastrukturu čini najkritičnijom i najranjivijom. Dva najpovezanija sustava u tom smislu jesu sustav električne energije o kojem ovise sve druge infrastrukture, dok on pak ovisi o komunikacijskom sustavu i obratno. Tako „ispad neke hidrocentrale ili termoelektrane neće negativno utjecati samo na energetski sektor, već i na informacijski, telekomunikacijski, gospodarski, financijski i cijeli niz uslužnih djelatnosti, ali isto tako vrijedi i obrnuto“ (Matika, 2009: 51).

Možda najveći problem s kojim se danas suočava sustav kritične infrastrukture jesu asimetrične prijetnje, u koje spadaju i kibernetičke prijetnje, a koje je, navode Klaić i Perešin (2012: 337), jako teško analitički predviđati i predvidjeti, zbog čega je teško razvijati i mehanizme njihove zaštite.

4.1.1. Troškovi napada na kritičnu informacijsku infrastrukturu

Kibernetički incidenti koji pogađaju kritičnu informacijsku infrastrukturu danas se smatraju globalnim rizicima koji mogu imati značajan negativni utjecaj na mnoštvo gradova i industrija u narednih 10 godina“ (Tofan i dr, 2016: 4, prema World Economic Forum, 2016: 11). Prema izvješću Tofan i dr (2016: 4), napadi na kritičnu informacijsku infrastrukturu najviše pogađaju financijski, sektor informacijsko-komunikacijskih tehnologija te energetski sektor.

Autori su u izvješću o troškovima napada na kritičnu informacijsku infrastrukturu objedinili ukupno 17 studija, od čega se njih šest odnosi na prostor Europske unije, a 11 na prostor van EU-a. Metode kojima su se autori pojedinih istraživanja koristili za izvlačenje podataka bili su ankete/upitnici (rasprostranjen alat, uglavnom u slučajevima u kojima su u istraživanje uključeni stručnjaci), analiza logova povezanih s cyber napadima koje su istraživale specijalizirane sigurnosne tvrtke te javno objavljeni podaci u medijima i otvorenim izvorima.

Kao najčešći tip napada na kritične sektore navode se DDoS napadi te maliciozni programi. U smislu nacionalnog gubitka zbog napada na informacijsku infrastrukturu, on doseže do 1,6 posto BDP-a u pojedinim europskim zemljama. Druge studije pak spominju gubitke od 425 tisuća do 20 milijuna eura po kompaniji godišnje. Jedna studija procjenjuje da je prosječni trošak cyber gubitaka po kompaniji varirao između 2,3 i 15 milijuna eura u 2015., dok druga studija procjenjuje da je ekonomski gubitak za globalnu ekonomiju između 330 i 506 milijardi eura. Države čije ekonomije trpe najveće štete zbog napada na informacijske sustave jesu SAD, Njemačka, Japan, Ujedinjeno Kraljevstvo, Australija i Rusija.

Tofan i dr. (2016: 5) zaključuju kako zemlje toleriraju zlonamjerne aktivnosti sve dok to ostaje na prihvatljivoj razini, manje od dva posto nacionalnog dohotka, a hitnost za pripremu i ulaganje u odgovor na sigurnosni incident obično se javljaju tek nakon događaja sa značajnim utjecajem. Također, poduzećima nedostaju kvalificirani zaposlenici, a problem je i što velika većina organizacija još uvijek nema implementirane osnovne sigurnosne kontrole. Istovremeno, napadači prilagođavaju i nadograđuju svoje tehnike, čineći ih još efikasnijima, dok se tvrtke bore sa starim taktikama.

4.1.2. Problematika informacijske infrastrukture u Republici Hrvatskoj

O povijesti kritične informacijske infrastrukture u Republici Hrvatskoj piše Majić (2016: 14). Kako pojašnjava, prije Domovinskog rata, informacijska infrastruktura u Hrvatskoj dijelila se na civilnu i vojnu komponentu. Nakon devedesetih, takva podjela napuštena je te je informacijska infrastruktura objedinjena, a za kompletnu komunikacijsku mrežu bila je nadležna tvrtka Hrvatska pošta i telekomunikacije (HPT).

Budući da je i komunikacija tijela državne uprave išla preko iste komunikacijske mreže, kada su se javne komunikacije privatizirale, sigurnost je stavljena u drugi plan. Postojala je ideja da državna tvrtka „Odašiljači i veze" izgradi državnu mrežu preko koje bi bila objedinjena infrastruktura svih državnih tvrtki, ali bi se ista tvrtka pojavila i u ulozi novog telekoma. O tome se raspravljalo u nekoliko navrata, ali ideja o državnoj mreži nikad nije realizirana. Kako se i izvještavalo u medijima[11], problem s funkcioniranjem DUZS-a i državnih institucija po pitanju komunikacijske mreže bio bi riješen kad bi Odašiljači i veze izgradili paralelni sustav optičkih kabela preko kojeg bi se odvijala komunikacija državne uprave. „Tako bi se na taj sustav mogle istovremeno spojiti sve telekomunikacijske kompanije i davati usluge za DUZS i ostale državne institucije, pa ako padne sustav jednog operatera, promet će ići preko druga dva" (Laušić, 2015). Međutim, tome se, logično, suprotstavila telekomunikacijska kompanija s najvećim brojem korisnika u Hrvatskoj (HT) pa je tako većina informacijske infrastrukture u Hrvatskoj i dalje u vlasništvu Nijemaca. Evidentno je da ta činjenica ne utječe povoljno na pitanje nacionalne sigurnosti u Hrvatskoj.

Odnosno, kako to dobro uočava Majić (2016: 14-15), „imajući na umu da je trenutni sustav, koji je sada u vlasničkoj strukturi stranaca, još uvijek osnovica na koju se priključuju bojišnički informacijsko-komunikacijski sustavi OSRH, sustavi MUP, kao i sustavi tijela državne vlasti, postavlja se pitanje sigurnosti i pouzdanosti sustava rukovođenja i zapovijedanja, a samim time i zaštite nacionalnih interesa, odnosno sigurnosti države. (...) U cilju poboljšanja stanja, utvrđivanja kritičke informacijske infrastrukture, neophodno je glavne komunikacijske čvorove i regionalna središta, kao i perspektivne lokacije za vojsku i

[11] Ipress.rtl.hr (2013) Veliki projekt Vlade: Objedinjavanje optičke infrastrukture, brzi internet za sve. 17. siječnja. http://ipress.rtl.hr/gospodarstvo/veliki-projekt-vlade-objedinjavanje-opticke-infrastrukture-brzi-internet-za-sve-25767.html Pristupljeno 15. veljače 2017.;

Tomić, Dražen (2014) [NAPOKON]: Objedinjena optička infrastruktura državnih firmi. *ICTbusiness.info*. 21 veljače. http://www.ictbusiness.info/telekomunikacije/napokon-objedinjena-opticka-infrastruktura-drzavnih-firmi Pristupljeno 15. veljače 2017.

policiju, sigurnosne službe i pojedina tijela državne vlasti, uvezati prijenosnim sustavom koji će biti ili u vlasništvu države ili određeni kao kritična informacijska infrastruktura“.

5. POLITIKA INFORMACIJSKE SIGURNOSTI U REPUBLICI HRVATSKOJ

Zakonska regulativa po pitanju informacijske i cyber sigurnosti u Republici Hrvatskoj, kao i zaštite kritične (informacijske) infrastrukture više je rezultat pritiska NATO-a i međunarodne zajednice, a manje vlastitih nastojanja i uviđanja potrebe za reguliranjem tih pitanja.

Kako zaključuju Klaić i Perešin (2011: 680), „usklađivanje dosadašnje nacionalne prakse u RH sa sigurnosnim smjernicama NATO-a i Europske unije, rezultiralo je donošenjem nacionalne regulative i postavljanjem temelja za implementaciju propisanih mjera i standarda informacijske sigurnosti u svim državnim tijelima, tijelima jedinica lokalne i područne (regionalne) samouprave, pravnim osobama s javnim ovlastima i drugim pravnim osobama koje u svom djelokrugu koriste klasificirane i neklasificirane podatke“. Međutim, da bi zakoni, strategije i pravilnici bili uspješno implementirani i da ne bi ostali tek „mrtvo slovo na papiru“, potrebno je pitanje cyber sigurnosti sagledati u kontekstu cijelog društva te na toj razini započeti s promjenama i osvještavanjem važnosti cyber problematike.

Opći koncept regulativnog okvira kakvog su predlagali Klaić i Perešin (2011: 686) sastoji se od kombinacije zakonodavnih propisa, međunarodnih i nacionalnih normi te unutarnjih standarda pojedine organizacije, bilo da je riječ o državnoj upravi ili privatnoj kompaniji.

Prema sigurnosnim informacijskim kriterijima, odnosno, aspektima informacijske sigurnosti, regulativni okvir kibernetičke sigurnosti podijelili su na regulativnu posebnih podatkovnih domena, sigurnosnu regulativu, regulativu privatnosti i regulativu odgovornosti. Pod regulativu posebnih podatkovnih domena spadaju klasificirani podaci, neklasificirani podaci, osobni podaci i intelektualno vlasništvo. Sigurnosnu regulativu čini regulativa kibernetičkog kriminala, tajnog nadzora komunikacija, kritične infrastrukture i kritične informacijske infrastrukture. (Klaić i Perešin, 2012: 351).

5.1. Hijerarhija propisa informacijske sigurnosti u državnom sektoru

Kada je riječ o hijerarhiji propisa informacijske sigurnosti u državnom sektoru, prema Klaić i Perešin (2011: 690) prve tri razine piramide čine implementacijski okvir (provedbene politike), unutar kojeg su zakoni, uredbe, pravilnici i interni akti te ostali dokumenti koje propisuju Ured Vijeća za nacionalnu sigurnost i savjetnici za informacijsku sigurnost u

tijelima, a slijede ih interni provedbeni akti u državnim tijelima te pravilnici Zavoda za sigurnost informacijskih sustava i Nacionalnog CERT-a. Sljedeća tri stupnja prema vrhu piramide čine legislativni okvir, odnosno, politike informacijske sigurnosti. Tu spadaju pravilnici Ureda Vijeća za nacionalnu sigurnost o sigurnosnim provjerama, fizičkoj sigurnosti i slično, potom Zakon o sigurnosno-obavještajnom sustavu RH, Zakon o sigurnosnim provjerama, Zakon o tajnosti podataka te Uredbe Vlade RH. Na vrhu piramide, kao dokument koji određuje strateške ciljeve, tada je bio Nacionalni program informacijske sigurnosti, čiju ulogu danas zamjenjuje Strategija kibernetičke sigurnosti Republike Hrvatske, kao krovni dokument.

5.2. Zakoni i propisi s područja informacijske sigurnosti u RH

Postoji čitav niz zakona, strategija, programa, akcijskih planova, pravilnika i uredbi koji na direktan ili indirektan način uređuju pitanje informacijske/cyber sigurnosti i kritične (informacijske) infrastrukture. U nastavku rada detaljnije će biti obrađeni samo najznačajniji propisi, važni za ovaj rad i daljnje istraživanje.

Tablica 1: Popis pravnih propisa s područja informacijske sigurnosti i kritične infrastrukture

STRATEGIJE, PROGRAMI, AKCIJSKI PLANOVI	**GODINA**
Nacionalni program informacijske sigurnosti u Republici Hrvatskoj	2005.
Nacionalna strategija kibernetičke sigurnosti i Akcijski plan za provedbu Nacionalne strategije kibernetičke sigurnosti	2015.
ZAKONI	**GODINA**
Zakon o potvrđivanju Konvencije o kibernetičkom kriminalu	2002.
Zakon o elektroničkoj ispravi	2005.
Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske	2006.
Zakon o informacijskoj sigurnosti	2007.
Zakon o tajnosti podataka	2007.
Zakon o sigurnosnim provjerama	2008.
Kazneni zakon	2011.
Zakon o izmjenama i dopunama Zakona o sigurnosnim provjerama	2012.
Zakon o izmjeni Zakona o tajnosti podataka	2012.
Zakon o zaštiti osobnih podataka	2012.
Zakon o kritičnim infrastrukturama	2013.
Zakon o pravu na pristup informacijama	2013.
Zakon o državnoj informacijskoj infrastrukturi	2014.
UREDBE	**GODINA**
Uredba o načinu označavanja klasificiranih podataka, sadržaju i izgledu	2007.

uvjerenja o obavljenoj sigurnosnoj provjeri i izjave o postupanju s klasificiranim podacima	
Uredba o sigurnosnoj provjeri za pristup klasificiranim podacima	2007.
Uredba o mjerama informacijske sigurnosti	2008.
Uredba o organizacijskim i tehničkim standardima za povezivanje na državnu informacijsku infrastrukturu	2015.
Uredba o preuzimanju Direktive 2013/40 EU o napadima na informacijske sustave te Direktive 2014/62 EU o kaznenopravnoj zaštiti eura i drugih valuta od krivotvorenja	2015.
PRAVILNICI I NAPUTCI	**GODINA**
Pravilnik o standardima organizacije i upravljanja područjem sigurnosti informacijskih sustava	2008.
Pravilnik o standardima organizacije i upravljanja područjem sigurnosti informacijskih sustava	2008.
Pravilnik o standardima sigurnosti poslovne suradnje	2008.
Naputak o provedbi sigurnosne akreditacije Sustava registara	2009.
Pravilnik o kriterijima za ustrojavanje radnih mjesta savjetnika za informacijsku sigurnost	2011.
Pravilnik o standardima fizičke sigurnosti	2011.
Pravilnik o standardima sigurnosne provjere	2011.
Pravilnik o standardima sigurnosti podataka	2011.
Pravilnik o metodologiji za izradu analize rizika poslovanja kritičnih infrastruktura	2013.
Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga	2013.
Pravilnik o izmjenama i dopunama Pravilnika o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga	2016.[12]

Izvor: autorica

5.2.1. Strategije nacionalne sigurnosti Republike Hrvatske (SNS) iz 2002. i 2017.

S obzirom na to da kibernetičke prijetnje u to vrijeme u Hrvatskoj nisu bile toliko uznapredovale, bivša SNS iz 2002. godine te se problematike spominje na tek dva mjesta. Pod izazovima, rizicima i prijetnjama Republici Hrvatskoj, u Strategiji se tako prepoznala i mogućnost ugrožavanja informatičkog sustava RH: „Stalno povećavanje korištenja informatičke tehnologije u javnoj i privatnoj sferi, praćeno je konstantnim povećanjem rizika kompjutorskoga kriminala i ugrožavanja informatičkih sustava. Na ovom području rizici nisu

[12]Kao relevantni uzeti su zakoni s područja informacijske sigurnosti koje su kao takve označili Ured vijeća za nacionalnu sigurnost (http://www.uvns.hr/hr/normativni-akti/informacijska-sigurnost); CERT (http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-04-110.pdf) te Međunarodna telekomunikacijska unija (http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf). Također, autorica je u obzir uzela i druge propise koje je tijekom izrade rada i istraživanja uočila kao relevantne.

samo u mogućnosti vanjskog ugrožavanja informatičkog sustava Republike Hrvatske, već i u mogućim zlouporabama privatnih podataka građana Republike Hrvatske od strane državnih tijela i institucija Republike Hrvatske, ili privatnih organizacija“ (Hrvatski sabor, 2002). Prijetnje koje bi mogle ugroziti informatički sustav RH spominju se i u četvrtom poglavlju, o unutarnjoj sigurnosti RH. Iako je već tada predviđen razvoj strategije, do operativnog provođenja te zamisli došlo je tek 13 godina kasnije i to pod pritiskom međunarodnih institucija i stručnjaka s područja cyber sigurnosti, a manje kao izraz političke volje za ozbiljnom pristupu ovom gorućem problemu.

Nešto optimističnije stanje po pitanju cyber sigurnosti je u novoj Strategiji nacionalne sigurnosti koju je Hrvatski sabor donio 14. srpnja 2017. godine. U njoj su priznali kako se paradigma sigurnosti promijenila te kako je mala vjerojatnost da će država doživjeti izravnu vojnu ugrozu. Kao puno veću prijetnju predstavili su hibridni rat, gospodarske i druge prijetnje.

Zbog toga bi, prema aktualnoj Strategiji nacionalne sigurnosti, svaka Vlada trebala s Predsjednikom države izraditi strategiju ili je ažurirati na samom početku svog mandata. Provedbu će, svake godine kroz izvješća, provjeravati Hrvatski sabor. Osim problema s novim valom migracija, klimatskim promjenama, demografskim kretanjima, priznali su kako se svijet mijenja zbog razvoja novih tehnologija, kao i činjenicu da internet ima sve važniju ulogu u kreiranju mišljenja i informiranju društva.

Iako informacijske tehnologije olakšavaju ljudima život, sve je više onih koji ih koriste zlonamjerno. Strategija nacionalne sigurnosti spominje da su u kibernetičkom prostoru granice nepoznate te su zbog toga ugroženi svi. Štete u tom svijetu itekako se mogu prenijeti na materijalni svijet pa priznaju da će u budućnosti sukobi biti takvi da neće biti moguće jasno razlučiti rat od mira.

U dokumentu stoji i kako smo mi, sami ili kao dio EU ili NATO-a, također ugroženi zbog nekonvencionalnog načina ratovanja. Također, širenjem uprave i zdravstva u online svijet postoji mogućnost zloupotrebe takvih informacija. Stoga za zaštitu društva smatraju da je nužna zaštita života, ljudi, dobara te osobito kritične infrastrukture. Kao najbolji način prevencije spominje se jačanje otpornosti infrastrukture i sustava nadzora i upravljanja. Kako bi to osigurali, planira se izrada novih dokumenata i zakona, kao i nova politika upravljanja i očuvanja infrastrukture u rukama države. Zbog toga bi se sustav zaštite trebao proširiti i na znanstvene ustanove i sve one koje rade u korist države. Zbog međunarodnih ugroza,

predlažu i međunarodnu suradnju u tim područjima. To se planira napraviti poboljšavanjem kibernetičke infrastrukture.

Država se obvezala zaštititi i razvijati zaštitu cjelokupne elektroničke komunikacijske infrastrukture. Uz to, planiraju ulagati i dalje u obrazovanje, kao i usvajanje novih znanja i tehnologija kako bi ostali konkurentni u odnosu na druge države. Plan je i kompletna digitalizacija javnih i državnih servisa kako bi se smanjila birokracija. Naravno, uz preduvjet da paralelno s time razvijaju i kibernetsku sigurnost takvih sustava.

5.2.2. Nacionalni program informacijske sigurnosti u RH (NPIS)

Ovaj strateški dokument prvi je uređivao pitanje informacijske sigurnosti u Republici Hrvatskoj. Donijela ga je Vlada Republike Hrvatske 2005. godine.

Nacionalni program informacijske sigurnosti sastoji se od 10 poglavlja u kojima se definira informacijska sigurnost, zahtjevi informacijske sigurnosti s aspekta međunarodnih odnosa, stanje informacijske sigurnosti u RH, razgraničenje nadležnosti u odnosu na podatke i informacijsku strukturu u RH, sigurnosna politika, edukacija i razvoj sigurnosne kulture te provedba NPIS-a. Važan aspekt NPIS-a za koji bismo iz današnje perspektive mogli reći da nije u cijelosti ispunjen te da je podbacio u implementaciji jest plan o edukaciji i razvoju sigurnosne kulture, za sve razine formalnog obrazovanja, ali i šireg građanstva.

„Sigurnosni standardi nisu tajna već temeljni zahtjev svakog radnog mjesta „od portira do predsjednika uprave“ u tvrtki te „od građanina do predsjednika“ u državi. Bez sigurnosne kulture nemoguće je provesti razvoj informacijskog društva. Potrebno je uvesti i stalno razvijati formalne informatičke obrazovne programe, od osnovnog, preko srednjeg pa do visokog školstva te obrazovnih programa prilagođenih za državnu upravu“ (SDUeH, 2005: 71).

Zaključno, NPIS je ipak bio uspješan kada je u pitanju institucionalno i pravno uređenje pitanja informacijske sigurnosti jer su upravo iz NPIS-a proizašli pojedini propisi koji su kasnije doneseni te nužne izmjene i dopune pojedinih zakona.

5.2.2. Nacionalna strategija kibernetičke sigurnosti

Dugo iščekivana Nacionalna strategija kibernetičke sigurnosti svjetlo dana ugledala je 7. listopada 2015. godine.[13] Njezina je svrha kontinuirano i temeljito provođenje niza aktivnosti koje su potrebne za razvoj i jačanje sposobnosti Hrvatske na području cyber sigurnosti i izgradnja sigurnog društva u današnjem, kibernetičkom prostoru. Da bi se takvo što postiglo, kao što je navedeno u strategiji, nužno je povezivanje i međusobno razumijevanje ove problematike u svih društvenim sektorima.

Kao osnovna načela pristupu kibernetičke sigurnosti, Nacionalna strategija kibernetičke sigurnosti vidi sveobuhvatnost, integraciju, proaktivni pristup, jačanje otpornosti, pouzdanosti i prilagodljivosti te primjenu zakona, razvoj usklađenog zakonodavnog okvira, primjenu načela supsidijarnosti i proporcionalnosti (Vlada RH, 2015: 6). Strategija bi se trebala implementirati u javnom, akademskom i gospodarskom sektoru te sektoru građanstva. Kao ciljevi navedeni su:

1. Sustavni pristup u primjeni i razvoju nacionalnog zakonodavnog okvira kako bi se uzela u obzir nova, kibernetička dimenzija društva
2. Provođenje aktivnosti i mjera u svrhu povećanja sigurnosti, otpornosti i pouzdanosti kibernetičkog prostora
3. Uspostavljanje učinkovitijeg mehanizma razmjene, ustupanja i pristupa podacima potrebnim za osiguravanje više razine opće sigurnosti u kibernetičkom prostoru
4. Jačanje svijesti o sigurnosti svih korisnika kibernetičkog prostora kroz pristup koji razlikuje specifičnosti javnog i gospodarskog sektora, pravnih i fizičkih osoba
5. Poticanje razvoja usklađenih obrazovnih programa
6. Poticanje razvoja e-usluga kroz razvoj povjerenja korisnika u e-usluge definiranjem odgovarajućih minimalnih sigurnosnih zahtjeva;
7. Poticanje istraživanja i razvoja u svrhu aktiviranja potencijala i poticanja usklađenog rada akademskog, gospodarskog i javnog sektora
8. Sustavni pristup međunarodnoj suradnji (Vlada RH, 2015: 7).

[13] Premda je vijest o donošenju Nacionalne strategije kibernetičke sigurnosti u Hrvatskoj (s pravom) dočekana kao velika i pozitivna, Hrvatska je jedna od zemalja koje su među zadnjima donijele takav akt. Prije nas učinila je to čak i Albanija, koja se u društvenom kontekstu gleda kao manje razvijena zemlja od Hrvatske. Podaci o tome kada je koja zemlja donijela Strategiju kibernetičke sigurnosti dostupni su na internetskim stranicama NATO-va *Zajedničkog centra izvrsnosti za pitanja cyber-obrane:* https://ccdcoe.org/cyber-security-strategy-documents.html.

Kao područja kibernetičke sigurnosti dobro su prepoznati elektronička komunikacijska infrastruktura i usluge, kritična komunikacijska i informacijska infrastruktura i upravljanje kibernetičkim krizama te kibernetički kriminal. Navedeni su i konkretni, pojedinačni ciljevi vezani uz određeno područje, bilo da je riječ o međunarodnoj suradnji ili tehničkoj koordinaciji u obradi računalnih sigurnosnih incidenata.

U Akcijskom planu za provedbu Strategije ciljevi su razrađeni kroz konkretne mjere, rokove, nositelje provedbe mjera te pokazatelje uspješnosti provedbe. Svojevrstan je kontrolni mehanizam provedbe Nacionalne strategije kibernetičke sigurnosti, kako ciljevi zapisani u njoj ne bi ostali tek na razini dobrih ideja i lijepih želja. U Akcijskom planu predviđene su 74 mjere za implementiranje informacijske sigurnosti na području javnih elektroničkih komunikacija, elektroničke uprave, elektroničkih financijskih usluga, kritične komunikacijske i informacijske infrastrukture i upravljanja krizama, kibernetičkog kriminaliteta, zaštite podataka, tehničke koordinacije u obradi računalnih sigurnosnih incidenata, međunarodne suradnje te obrazovanja, istraživanja, razvoja i jačanja svijesti o sigurnosti u kibernetičkom prostoru.

Predviđeno je da se nadzor provedbe nad Akcijskim planom provodi putem izvješća koja su nositelji mjera dužni podnositi Nacionalnom vijeću za kibernetičku sigurnost. Rok za provedbu pojedinih mjera bio je primjerice, pola godine od dana donošenja Strategije, ali simptomatično je da su odgovorna tijela predviđena Nacionalnom strategijom kibernetičke sigurnosti (Nacionalno vijeće za kibernetičku sigurnost i Operativno-tehnička koordinacija za kibernetičku sigurnost) osnovana tek u lipnju 2016. Neobična je i činjenica da se vladajućim elitama koje su se smjenjivale na vlasti, osam mjeseci nije žurilo donijeti odluku o osnivanju tih tijela, a onda ih je naprasno donijela tehnička Vlada Tihomira Oreškovića nekoliko tjedana prije no što će otići s vlasti. Prema Odluci o njihovom osnivanju, u svakom od tih tijela, zaduženim za daljnje praćenje stanja sigurnosti kibernetičkog prostora i provođenja strategije, sjedit će po jedan predstavnik iz nekolicine ministarstava, te predstavnici Sigurnosno-obavještajne agencije, UVNS-a, DUZS-a, OTC-a, CARNET-a, itd.

Hoće li ovi dokumenti zaživjeti i u stvarnosti ili će u svom provođenju ostati tek na deklarativnoj razini, tek ostaje za vidjeti. Pojedini stručnjaci nisu optimistični glede stvarne implementacije Strategije. Kako navodi Brzica (2015: 35), „poučeni lošim iskustvima, kao što je slučaj sa Zakonom o kritičnim infrastrukturama i nikad ostvarenim zadaćama od kojih neke (popis kritične infrastrukture) izravno utječu na provedbu Strategije i Akcijskog plana kibernetičke sigurnosti, Vlada mora zaista biti proaktivna u ostvarivanju svojih deklariranih

ciljeva“. S obzirom na političku nestabilnost kojoj zadnjih godinu dana svjedočimo u Hrvatskoj, zaista je upitno u kojoj mjeri i postoji li uopće politička volja za pitanjem kibernetičke sigurnosti ili će se ona odjednom probuditi tek kada nam svima počne *gorjeti za petama*. Kao što to stručnjak za sigurnost Zvonko Orehovec dobro uočava po pitanju neosmišljavanja Strategije nacionalnog razvoja RH, ista se paralela i zaključci mogu povući i po pitanju provedbe ovih strateških dokumenata. Problem je što „svaka nova vlada koja dođe na vlast negira postignuća prethodne i počinje iznova pisati strategije“ koje nisu sinkronizirane s drugim strategijama i propisima te dolazi do velikog nesklada, što autor pripisuje „vrlo niskoj sigurnosnoj kulturi naših političara“ (Orehovec, 2016: 28).

5.2.3. Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske

Ovim Zakonom, donesenim 2006. godine, osnovane su Sigurnosno-obavještajna agencija (SOA) i Vojna sigurnosno-obavještajna agencija te Zavod za sigurnost informacijskih sustava. Zakon je za informacijsku sigurnost važan jer definira Ured Vijeća za nacionalnu sigurnost (UVNS) kao „središnje državno tijelo odgovorno za utvrđivanje i provedbu aktivnosti vezanih za primjenu mjera i donošenje standarda informacijske sigurnosti u državnim tijelima u Republici Hrvatskoj“ (Hrvatski sabor, 2006). Zakon o sigurnosno-obavještajnom sustavu također propisuje da UVNS izdaje certifikate za obavljene sigurnosne provjere. Istim Zakonom definirane su i zadaće pojedinih tijela važnih za provođenje informacijske sigurnosti u RH.

5.2.4. Zakon o informacijskoj sigurnosti

Zakonom o informacijskoj sigurnosti iz srpnja 2007. uređeni su „pojam informacijske sigurnosti, mjere i standardi informacijske sigurnosti, područja informacijske sigurnosti, nadležna tijela za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti“ (Hrvatski sabor, 2007). Prema njemu, mjere i standardi informacijske sigurnosti obuhvaćaju način postupanja s klasificiranim podacima te postupanje prilikom neovlaštenog pristupanja tim podacima. Kao područja informacijske sigurnosti, u Zakonu su navedeni sigurnosna provjera, fizička sigurnost i sigurnost podataka. Također je precizirana zadaća Nacionalnog CERT-a te odgovorna tijela za provedbu i nadzor informacijske sigurnosti (savjetnici za informacijsku sigurnost).

5.2.5. Zakon o tajnosti podataka

Zakonom su uređeni stupnjevi tajnosti, pojam klasificiranih i neklasificiranih podataka, pristup tim podacima te njihova zaštita i nadzor. Pod klasificiranim podatkom podrazumijeva se onaj koji je nadležno tijelo označilo takvim i za koji je utvrđen stupanj tajnosti (vrlo tajno, tajno, povjerljivo, ograničeno) ili ga je kao takvog predala neka od zemalja ili institucija s kojima Republika Hrvatska surađuje. Za razliku od klasificiranih podataka, neklasificirani nemaju utvrđen stupanj tajnosti, ali se koriste u službene svrhe i dostupni su ograničenom broju ljudi (Hrvatski sabor, 2007).

5.2.6. Kazneni zakon

Kazneni zakon iz 2011. u smislu cyber sigurnosti definira pojmove kao što su računalni sustav, računalni podatak i računalni program. Novina u tom Kaznenom zakonu, za razliku od starih je što postoji posebna glava (XXV.) koja se bavi kaznenim djelima protiv računalnih sustava, programa i podataka. U tom djelu Zakona opisana su kaznena djela cyber kriminala koja Hrvatska kriminalizira te predviđene kazne. U to se ubrajaju: neovlašteni pristup, ometanje rada računalnog sustava, oštećenje računalnih podataka, neovlašteno presretanje računalnih podataka, računalno krivotvorenje, računalna prijevara, zlouporaba naprava, teška kaznena djela protiv računalnih sustava, programa i podataka.

5.2.7. Zakon o kritičnim infrastrukturama

Zakon o kritičnim infrastrukturama uređuje pitanja „nacionalne i europske kritične infrastrukture, sektore nacionalnih kritičnih infrastruktura, upravljanje kritičnim infrastrukturama, izradu Analize rizika, Sigurnosni plan vlasnika/upravitelja, sigurnosnog koordinatora za kritičnu infrastrukturu, postupanje s osjetljivim i klasificiranim podacima te nadzor nad provedbom Zakona“ (Hrvatski sabor, 2013). Definirani su i sektori nacionalne kritične infrastrukture te međusektorska mjerila koja procjenjuju učinak prekida rada kritične infrastrukture (s obzirom na ljudske i gospodarske gubitke i utjecaj na javnost). Također, Zakonom je predviđena kazna od pola milijuna kuna ako se ne izradi Analiza rizika kritičnih infrastruktura i ne popiše sva kritična infrastruktura u Hrvatskoj (što je klasificirani podatak).

5.2.8. Zakon o državnoj informacijskoj infrastrukturi

Rokovi informatizacije i načela razvitka državne informacijske infrastrukture definirani su Zakonom o državnoj informacijskoj infrastrukturi. Taj Zakon uređuje upravljanje javnim registrima, bazama podataka, središnjim državnim portalom te sustavima poput e-Građana. Načela razvitka državne informacijske infrastrukture obvezuju i na usklađivanje projekata informatizacije s europskim normama.

5.3. Norme informacijske sigurnosti

Kada je riječ o normama informacijske sigurnosti, najpoznatije su ISO (*International Organization for Standardization*) norme, osobito ISO/IEC 27001. Ta norma definira kako implementirati i upravljati Sustavom upravljanja informacijskom sigurnošću (ISMS - *Information Security Management System*), što je važno i za građenje cyber sigurnosti jer ISO 270001 nudi katalog od 133 sigurnosne kontrole te definira okvir za detekciju sigurnosnih problema (Košutić, 2012: 42-43).

Općenito gledano, norme „predstavljaju rješenje zajedničkih potreba državne uprave i gospodarstva za jedinstvenim sustavima, primjerice u području upravljanja sigurnošću informacija (HRN ISO/IEC 27001) ili u području vrednovanja informacijske tehnologije (ISO/IEC 15408). Norme predstavljaju obvezujuće dokumente, ali isključivo u slučajevima kada na njih upućuju odredbe nekog zakonskog propisa“ (Klaić i Perešin, 2011: 692). Važnost ISO 270001 norme je u njezinoj sveobuhvatnosti jer katalog od sigurnosnih kontrola ne uključuje samo IT sigurnost, već i čitav spektar drugih mjera koje se potrebne da bi se u nekoj tvrtki, organizaciji ili državnoj upravi postigla zavidna razina informacijske/cyber sigurnosti. To se osobito tiče organizacijskih mjera, fizičke i pravne zaštite, ali i adekvatnog upravljanja ljudskim resursima, odnosno, pametnog odabira i provjere zaposlenika koji barataju s informacijama.

5.4. Institucionalni okvir

Kada je riječ o institucionalnom okviru informacijske sigurnosti, u obzir treba uzeti domaća, ali i strana tijela u kojima je Hrvatska članica ili s kojima surađuje.

5.4.1. Tijela informacijske sigurnosti u RH

Najvažnija tijela vezana uz informacijsku sigurnost u Republici Hrvatskoj jesu: Ured Vijeća za nacionalnu sigurnost (UVNS), Zavod za sigurnost informacijskih sustava (ZSIS), Nacionalni CERT, Odjel za visokotehnološki kriminalitet, Agencija za podršku informacijskim sustavima i informacijskim tehnologijama, Agencija za zaštitu osobnih podataka te Uprava za e-Hrvatsku.

a) Ured Vijeća za nacionalnu sigurnosti (UVNS)

Ured Vijeća za nacionalnu sigurnost središnje je državno tijelo za informacijsku sigurnost. On koordinira, usklađuje i nadzire primjenu mjera koja se tiču informacijske sigurnosti te mjera u okviru sigurnosne provjere, fizičke sigurnosti i sigurnosti podataka. U sklopu toga izdaje certifikate za pristup domaćim, europskim i NATO-vim klasificiranim podacima. U sklopu Ureda djeluje i Središnji registar koji je zadužen za cjelovitu klasifikaciju podataka. Njegovi zaposlenici koordiniraju međunarodnu suradnju te nakon odluka Vlade zaključuju sigurnosne ugovore za zaštitu klasificiranih podataka.

b) Zavod za sigurnost informacijskih sustava

Zavod za sigurnost informacijskih sustava (ZSIS) središnje je državno tijelo koje radi na standardima sigurnosti informacijskih sustava, sigurnosnim akreditacijama informacijskih sustava, upravljanju kriptomaterijalima te koordinaciji prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava. Radom Zavoda za sigurnost informacijskih sustava upravlja ravnatelj kojeg imenuje i razrješuje Vlada Republike Hrvatske. U poslovima akreditiranja i izdavanja preporuka surađuju s ostalim agencijama i državnim tijelima.

c) Nacionalni CERT

Nacionalni CERT organizacija je koja se bavi očuvanjem informacijske sigurnosti u Hrvatskoj te koja obrađuje prijavljene incidente, ako jedna od strana u incidentu ima .hr domenu ili IP adresu unutar državnih granica (CERT, 2017). U okviru svog djelovanja provodi prevenciju napada te često objavljuje podatke o novim ugrozama te kako se od njih zaštititi. U sklopu tih akcija pokrenuli su i stranicu antibot.hr na kojoj građani mogu provjeriti je li njihovo računalo zaraženo te korišteno kao bot. Jednom godišnje objavljuju izvješće o stanju informacijske sigurnosti u zemlji.

d) Odjel za visokotehnološki kriminalitet

Odjel za visokotehnološki kriminalitet djeluje unutar Ministarstva unutarnjih poslova. Prati, analizira i rješava kaznena djela u domeni kibernetičkog kriminala. Osim toga, njegovi malobrojni zaposlenici obavljaju forenzičku analizu i nadzor interneta te pomažu drugim dijelovima MUP-a. Trude se izrađivati programe obuke novih policajaca za kibernetički kriminal te izrađuju i vlastita izvješća o kriminalu.

5.4.2. Međunarodna tijela informacijske sigurnosti

Domaća tijela usklađuju svoje postupke s preporukama međunarodnih agencija. Većina međunarodnih agencija bavi se obranom informacijskih sustava te na tome temelje svoj rad. Jedna od takvih je CERT EU koji priprema i odgovara na cyber napada na institucije Europske unije. Unutar njih razmjenjuje dobre prakse kako bi se povećala razina sigurnosti.

a) Agencija Europske unije za mrežnu i informacijsku sigurnost (ENISA)

Agencija Europske unije za mrežnu i informacijsku sigurnost (*European Network and Information Security Agency – ENISA*) daje savjete Europskoj komisiji i državama članicama EU o svim aspektima problema iz svog naziva. Posebno radi na procjeni mogućih rizika te njihovom rješavanju. Djelatnici agencije brinu se i za postavljanje nacionalnih CERT-ova koji preuzimaju prakse i prate razvoj sigurnosti i napada u pojedinim zemljama.

b) Europski centar za cyber kriminal

Zbog učestalih napada, ali i procesuiranja kriminalaca, osnovan je i Europski centar za cyber kriminal koji je zadužen za ukupno smanjivanje cyber kriminala. Rad su usmjerili na hvatanje organiziranih grupa koje napadaju kritičnu infrastrukturu i zadaju velike štete na sustavima. Unutar centra radi i J-CAT (*Joint Cybercrime Action Taskforce*), zajednička akcijska radna skupina koja koristi stručnost policije i istražitelja unutar i van granica EU u međunarodnim istragama. Tu je i *Eurojust*, institucija koja obučava tijela za provedbu zakona, ali i tužitelje za usuglašavanje procedura kod istraga cyber kriminala.

c) Europska obrambena agencija (EDA)

Za „borbeni“ dio cyber sigurnosti brine Europska obrambena agencija (*European Defence Agency – EDA*) koja promiče i razvija obrambenu i istraživačku tehnologiju. Oni razvijaju zajedničku platformu za odgovor na cyber napade. Kako bi to napravili, organiziraju i razne vježbe kriznog upravljanja unutar EU. Europskim zemljama pomaže i NATO čije se članice zajedno obučavaju za zonu cyber sigurnosti i ratovanja. Koncept njihove cyber obrane predložila je Estonija 2004. te su nakon toga formirani mnogi centri diljem Europe. Planiraju se otvoriti i novi centri cyber obrane u Sloveniji i Bugarskoj.

6. ISTRAŽIVANJE

6.1. Svrha i ciljevi istraživanja

Svrha je ovog istraživanja utvrditi u kojoj su mjeri pokriveni različiti parametri informacijske sigurnosti u tvrtkama čiji se sektori djelatnosti poklapaju sa sektorima kritičnih infrastruktura. Cilj je utvrditi koje su (organizacijske i tehničke) slabosti na kojima bi tvrtke trebale poraditi kako bi učinkovitije zaštitile svoju informacijsku/cyber sigurnost i prevenirale moguće direktne i indirektne ugroze nacionalne sigurnosti.

6.2. Metode istraživanja

Pitanje cyber sigurnosti samo je po sebi dovoljno kompleksno i teško za istražiti. S obzirom na to da se analiziraju prijetnje i rizici cyber sigurnosti kroz konkretne slučajeve, nije moguće samo matematički ili pak samo opisno odraditi analizu, već je potrebno koristiti različite metode i pristupe. Upravo zbog toga, u ovom radu kombinirat će se studija slučaja s GAP analizom, odnosno, analizom rascjepa ISO/IEC 27001:2013 normi. Lamza Posavec (2006) studiju slučaja definira kao „istraživačku metodu kojom se nastoje zabilježiti podrobne i obuhvatne informacije o jednom ili više pojedinačnih slučajeva određene skupine ili kategorije pojava te na temelju toga donositi zaključke o svim slučajevima iste kategorije“.

U prvom dijelu rada analiziraju se regulativni i institucionalni okvir vezan uz tematiku te trenutno stanje na području informacijske/cyber sigurnosti u Hrvatskoj i svijetu. Drugi dio rezerviran je za diferencijalnu (GAP) analizu postojećeg stanja i potreba u implementaciji sustava upravljanja informacijskom sigurnošću prema ISO/IEC 270001:2013 normi. Prema definiciji Cambridgevog instituta[14], GAP analiza je metoda koja se sastoji od definiranja postojećeg i željenog stanja kojem neka organizacija teži te jaza među njima. Da bi se taj jaz premostio, potrebno je ustanoviti koji je korake potrebno poduzeti na putu do cilja.

U konkretnom slučaju, kroz analizu četiri tvrtke, među kojima su tri javne zdravstvene ustanove i jedne energetske kompanije, GAP analizom želi se provjeriti koliki je raskorak između njihovih ciljeva na području informacijske sigurnosti i trenutnog stanja te koje su sigurnosne procedure i mjere zaštite dosad implementirali, a koje im nedostaju.

[14] University of Cambridge – Institute for Manufacturing. (2017) Gap analysis. http://www.ifm.eng.cam.ac.uk/research/dstools/gap-analysis/. Pristupljeno 12. veljače 2017.

GAP analiza ukazuje na to koliko je daleko neka tvrtka od ISO 27001 zahtjeva i kontrola te kako navodi Košutić (2017), „ona nije ništa drugo doli čitanje svake stavke ISO 27001 i analiziranja je li tu mjera implementirana u nekoj organizaciji“.

U konkretnom slučaju, GAP analiza provest će se po uzoru na istraživanje Dejana Košutića (2009) o primjeni normi informacijske sigurnosti na primjeru HEP-a. Za potrebe GAP analize u dvije tvrtke provest će se intervjui/upitnici s odgovornim osobama zaduženima za sigurnost, informacijske tehnologije, ljudske resurse i pravne poslove. Pitanja će biti generirana i oblikovana iz ISO/IEC 27001:2013 i ISO/IEC 27002:2013 standarda, a zbog opsega rada obuhvatit će sljedećih 10 poglavlja: Sigurnosna politika, Organizacija informacijske sigurnosti, Sigurnost vezana uz osoblje, Upravljanje resursima/imovinom, Fizička sigurnost i sigurnost u okruženju, Operativna sigurnost/sigurnost radnih operacija, Sigurnost komunikacija, Upravljanje incidentima narušavanja informacijske sigurnosti, Aspekti informacijske sigurnosti u okviru upravljanja kontinuitetom poslovanja i Usklađenost.

Zbog zaštite interesa kompanija koje će sudjelovati u istraživanju, u radu se neće spominjati njihova imena, već tek osnovni podaci o veličini ustanove, odnosno tvrtke i županiji u kojoj djeluje. Odabir ustanova i tvrtki vršit će se prema stupnju međuovisnosti kritičnih infrastruktura. Drugim riječima, u istraživanju će sudjelovati tvrtke u kojima bi, u slučaju ugrožavanja informacijske sigurnosti posredno ili neposredno, bila ugrožena i nacionalna sigurnost, budući da njihova djelatnost spada u sektor kritičnih infrastruktura.

U istraživanju će se koristiti kontrolni popis usklađenosti, po uzoru na standardizirane popise koji su u službenoj uporabi tvrtki[15] koje se komercijalno bave GAP analizom. Kroz pitanja o ISO normama cilj je ustanoviti na kojoj je razini informacijska sigurnost u tvrtkama koje čine uzorak istraživanja. Kako bi se dobila cjelokupna slika te daljnje preporuke po pitanju implementacije informacijske sigurnosti, to je moguće jedino kroz sveobuhvatnu analizu prethodno navedenih područja (informacijske tehnologije, ljudskih resursa, itd.). Za svaku pojedinu mjeru koju ISO standard propisuje, provjerava se je li implementirana u ustanovi i u kojoj mjeri. Odgovori će se kategorizirati prema sljedećoj skali (Košutić, 2009):

[15]Halkyn Consulting (2013) ISO27001 compliance checklist available for download. http://www.halkynconsulting.co.uk/a/2013/10/iso27001-compliance-checklist/. Pristupljeno 10. travnja 2017. / ISO27k Forum (2016) Documenation and records required for ISO/IEC 27001 certifiction. http://www.iso27001security.com/ISO27k_ISMS_Mandatory_documentation_checklist_release_1.docx. Pristupljeno 10. travnja 2017.

1. Sigurnosna mjera nije primjenjiva jer ne postoji rizik i zakonska odredba zbog koje bi mjera bila potrebna (oznaka „n/p“)
2. Sigurnosna mjera nije u planu ili nije provedena (oznaka 1 – provedena 0 %)
3. Sigurnosna mjera planirana je, ali nije provedena ili je pak provedena samo u teoriji, odnosno, na papiru, ali ne i u praksi (oznaka 2 – provedena 25 %)
4. Sigurnosna je mjera djelomično provedena, ali bez značajnijih efekata (oznaka 3 – provedena 50 %)
5. Sigurnosna mjera provedena je u potpunosti ili većim dijelom, ali problem je u nadzoru i doradi mjere, koji se ne provode na adekvatan način (oznaka 4 – provedena 75 %)
6. Sigurnosna mjera u potpunosti je provedena, kao i nadzor, dorada i mjerenje (oznaka 5 – provedena 100 %).

Na kraju će se usporediti rezultati iz upitnika prema područjima istraživanja (organizacija informacijske sigurnosti, sigurnosna politika, upravljanje resursima, fizička sigurnost, itd.) te na temelju toga donijeti ukupna ocjena informacijske sigurnosti.

6.3. Istraživačka pitanja

S obzirom na veličinu uzorka u ovoj GAP analizi, od ukupno četiri pravne osobe, odnosno tvrtke, nije realno postavljati hipoteze koje bi bile primjenjive na društvo u cijelosti, odnosno, na cjelokupnu problematiku koja se ovim radom želi istražiti. Stoga su u radu postavljena sljedeća istraživačka pitanja na koja se želi naći odgovor:

- Koje je generalno stanje sigurnosti u zdravstvenim ustanovama, a koje u energetskim tvrtkama?
- Kako poboljšati stanje informacijske sigurnosti u tvrtkama obuhvaćenim uzorkom?
- Koje su kratkoročne, a koje dugoročne mjere koje je potrebno poduzeti kako bi se informacijska sigurnost u tvrtkama povećala?
- Koji su glavni problemi vezani uz informacijsku sigurnost u ustanovama/tvrtkama koje su dio kritične infrastrukture Republike Hrvatske?

6.4. Moguća ograničenja prilikom istraživanja

Budući da je uzorak istraživanja namjeran i ograničen, sukladno zainteresiranosti ustanova i tvrtki za sudjelovanjem, rezultati se neće moći generalizirati na razini cjelokupnog sustava. Također, u obzir se mora uzeti i moguća ograničenost/nedostatak znanja i kompetentnosti za adekvatan odgovor na sva pitanja, s obzirom na osobe različitih profila koje će pojedina ustanova/kompanija dati.

6.5. Provedba istraživanja

Poziv na sudjelovanje u istraživanju odaslan je na ukupno 13 javnih zdravstvenih ustanova, pet privatnih poliklinika, tri energetske kompanije s pripadajućim tvrtkama kćerima i još toliko tvrtki iz sektora IT-a. Anonimiziran popis kontaktiranih ustanova i tvrtki dostupan je u Prilogu 1. Od toga, istraživanje je realizirano u tek tri javne zdravstvene ustanove s područja Grada Zagreba i Krapinsko-zagorske županije koje u prosjeku imaju između 600 i 1000 zaposlenika te jednoj većoj energetskoj kompaniji. U svakoj od kompanija strukturirani intervjui bili su sastavljeni od 34 stranice pitanja te su provedeni s ukupno osam osoba (po dvije osobe u svakoj). Intervjuirani su voditelji informatičkih službi, eksperti za sigurnost te osobe iz pravnih i kadrovskih poslova. Ovisno o ustanovi, razgovori su trajali u prosjeku između tri i šest sati. U daljnjoj analizi zdravstvene ustanove iz Grada Zagreba bit će označene kao Bolnica 1 i Bolnica 2, dok će zdravstvena ustanova iz Krapinsko-zagorske županije biti definirana kao Bolnica 3. Već sam nedostatak interesa za sudjelovanjem u istraživanju može ukazivati na manjak svijesti o informacijskoj sigurnosti unutar velikih sustava.

Analizirano je 10 poglavlja iz Annexa A ISO/IEC 27001:2013 standarda informacijske sigurnosti, dok su četiri poglavlja[16] izostavljena jer za rad i kontekst ustanova i tvrtki nisu toliko relevantna te su pojedina pitanja iz njih obuhvaćena obrađenim poglavljima. Analiza je razdvojena na zdravstvene ustanove i energetsku kompaniju. Zdravstvene ustanove bit će zajednički obrađene po analiziranim poglavljima, a pojedinačni rezultati za svaku od kontrola u pojedinoj bolnici dostupni su u Prilogu 2. Rezultati istraživanja u energetskoj kompaniji bit će kratko analizirani u zasebnom poglavlju.

[16] Riječ je o poglavljima vezanim uz kontrolu pristupa, odnose s dobavljačima, nabavku, razvoj i održavanje informacijskih sustava i kriptografiju.

7. ANALIZA USKLAĐENOSTI ZDRAVSTVENIH USTANOVA I ENERGETSKE KOMPANIJE S ISO/IEC 27001 STANDARDOM

7.1. Zdravstvene ustanove

Kao dva najveća uzroka svih sigurnosnih problema u zdravstvenim institucijama, djelatnici i ravnatelji isticali su manjak financijskih sredstava i potkapacitiranost osoblja. Točnije, kako je ravnatelj jedne bolnice rekao, „država nam nikad dosad nije dala niti kune za sigurnost“. Stanje nije daleko od istine, ako je suditi prema proračunu[17] Ministarstva zdravstva za 2017. i projekcijama za 2018. i 2019. godinu. Za općenitu informatizaciju, u koju spada obnavljanje licenci i ulaganje u računalne programe utrošit će se šest milijuna kuna. Troškovi integriranog planiranja odgovora, incidentna i krizna stanja iznosit će 100 tisuća kuna, dok detaljna raspodjela proračunskih sredstava po pojedinim bolnicama ne predviđa utrošak tih sredstava za računalne namjene. Dapače, u tim su stavkama zaista poredane nule. Ne čudi to, jer se zadnjih mjeseci u bolnicama teško nalazi sredstava i za liječenje bolesne djece[18], a kamoli ulaganje u sigurnost. Iz budžeta kojima raspolažu ravnatelji hrvatskih bolnica, čak 70-90 posto sredstava odlazi na plaće zaposlenika te je evidentno da se u sigurnost nema otkuda uložiti. Nije to problem rezerviran samo za hrvatski zdravstveni sustav, već na njega kao na glavni problem u svom istraživanju[19] sigurnosti bolnica nailaze i američki istraživači iz Independent Security Evaluators. Zbog svega toga, za očekivati je rezultate koji slijede u nastavku rada, a koji unatoč pojedinim brojčano prihvatljivim ocjenama, ukazuju na to da zdravstvene ustanove imaju još puno toga za napraviti po pitanju sigurnosti. Primjerice, ne bi se smjelo dogoditi da u 21. stoljeću jedna bolnica rezervne kopije podataka drži u server sobi, kao što je to slučaj s jednom od zdravstvenih ustanova u kojoj je provedeno istraživanje.

---

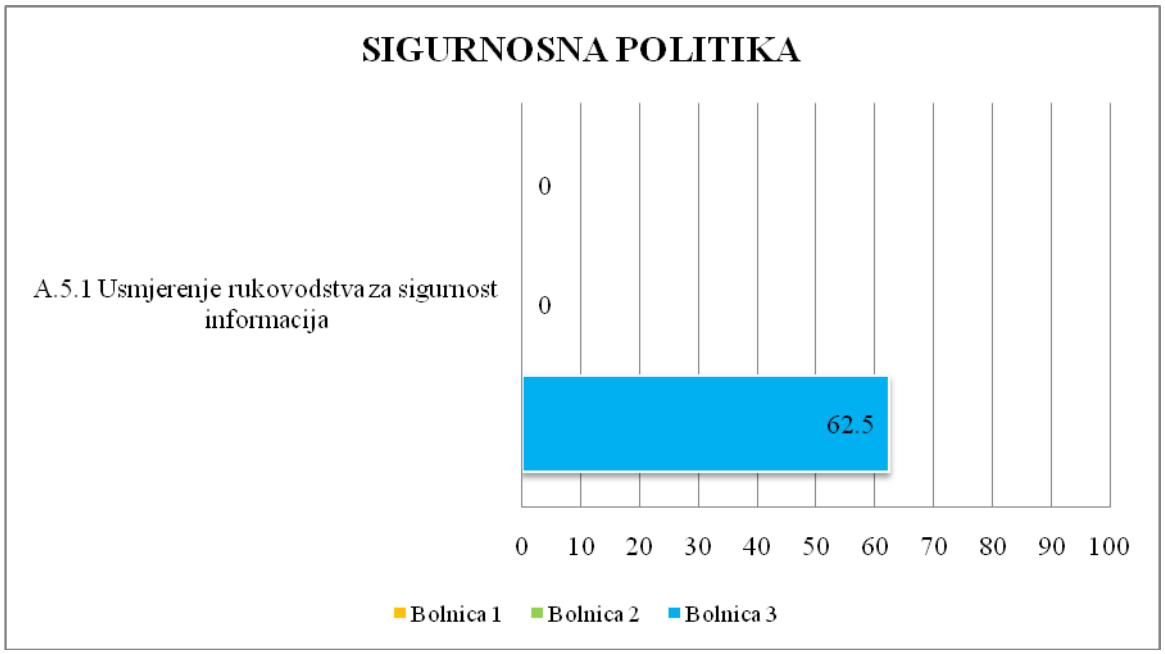
[17] Ministarstvo zdravstva – državni proračun za 2017-2019. godine. https://zdravlje.gov.hr/UserDocsImages//2017%20Financijski%20planovi%20i%20strate%C5%A1ki%20dokumenti,%20javna%20nabava//MINISTARSTVO%20ZDRAVSTVA%20%20-%20DR%C5%BDAVNI%20PRORA%C4%8CUN%20ZA%20%202017%20-%202019%20%20GODINE.xlsx. Pristupljeno 10. lipnja 2017.

[18] Slučajevi sedmero djece iz Klinike za dječje bolesti u Zagrebu za koje bolnica nije imala novac za skupi lijek koji im može produljiti život, u lipnju i srpnju ove godine punio je novinske stupce i internetske portale u Hrvatskoj. O tome je izvještavao i Index.hr (2017) Klaićeva nema novca: Sedmero djece neće dobiti lijek koji im može produžiti život. http://www.index.hr/black/clanak/klaiceva-nema-novca-sedmero-djece-nece-dobiti-lijek-koji-im-moze-produziti-zivot/976469.aspx. Pristupljeno 13. lipnja 2017.

[19] Riječ je o istraživanju Independent Security Evaluators (2016). Securing Hospitals: A research study and blueprint. https://securityevaluators.com/hospitalhack/. Pristupljeno 10. lipnja 2017. Studija je obuhvatila 12 zdravstvenih ustanova i šest medicinskih centara i platformi.

7.1.1. Usklađenost poglavlja „Sigurnosna politika“ u zdravstvenim ustanovama

Grafikon 1: Rezultati GAP analize za poglavlje "Sigurnosna politika"



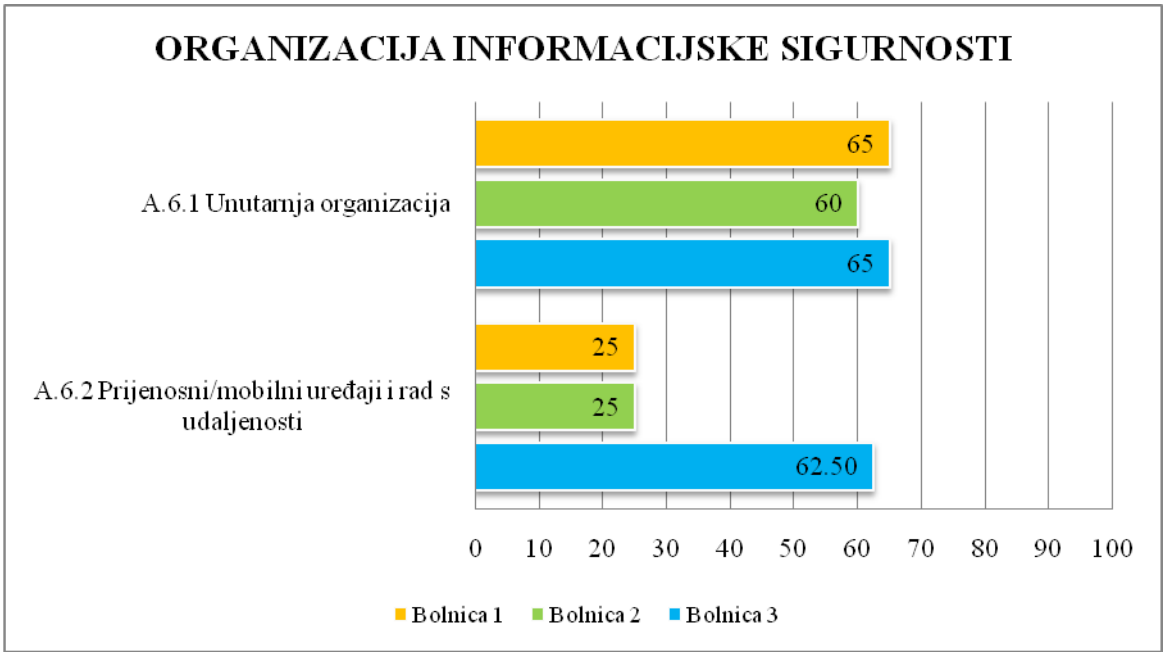
Izvor: autorica

Prema ISO/IEC 27001: 2013 standardu, prva kontrola odnosi se na objedinjavanje ciljeva i strategije informacijske sigurnosti kroz zajednički dokument kojem bi zeleno svijetlo trebalo dati rukovodstvo neke institucije ili tvrtke. Sigurnosnu politiku u tom smislu, pokazalo se istraživanjem, ima tek Bolnica 3. Riječ je o dokumentu koji datira iz 2007., a koji je u dogovoru s tom zdravstvenom institucijom za njih oblikovao isporučitelj mrežne i računalne opreme, a oni su na sebe preuzeli daljnje dopune i revizije. Dokument definira da je bolnica otvorena prema internetu, da se pristup štiti vatrozidom i sigurnosnim softverima, da je mreža segmentirana, da se radi *backup* podataka i slično. Niže politike koje bi dopunjavale krovnu politiku informacijske sigurnosti, a kao što su politika kontrole pristupa, klasifikacije informacija, fizičke sigurnosti i sigurnosti u okruženju, prijenosa informacija i drugih, ne postoje kao zasebni dokumenti. Međutim, kako su istaknuli u Bolnici 3, o nižim politikama postoje nepisana pravila koja se primjenjuju za zaštitu informacijske sigurnosti institucije. Politika informacijske sigurnosti nekoliko je puta revidirana i dopunjavana, kako se mijenjao koncept i poslovanje bolnice. Primjerice, sustav je inicijalno bio zamišljen kao zatvoren, sa samo određenim dotičnim točkama prema internetu, kao što su bankarsko poslovanje, komunikacija e-mailovima i slično, ali kako je došlo do integracije Bolnice 3 i HZZO-a, uveli su nove servise, kao što su e-liste čekanja i e-uputnice, za što je trebalo mrežu

otvoriti prema internetu, te je samim time mijenjan i dokument koji regulira to područje. Za dokument politike informacijske sigurnosti zadužen je voditelj informatičke službe. Prije odobravanja i izmjene dokument ne prolazi kroz ruke rukovodstva, što je jedan od uvjeta u ISO standardu. Također nije niti iskomuniciran prema zaposlenicima i vanjskim stranama. Bolnica 1 i Bolnica 2 politiku informacijske sigurnosti nisu implementirale niti je smatraju potrebnom.

7.1.2. Usklađenost poglavlja „Organizacija informacijske sigurnosti“ u zdravstvenim ustanovama

Grafikon 2: Rezultati GAP analize za poglavlje „Organizacija informacijske sigurnosti“



Izvor: autorica

Odgovornosti i uloge vezane uz informacijsku sigurnost u Bolnici 2 definirane su unutar Pravilnika o unutarnjem ustrojstvu, sukladno opisu pojedinog radnog mjesta, ali su i dalje pretežito vezane uz uži dio informatičke sigurnosti. U preostale dvije zdravstvene ustanove ne postoji pisani dokument o tome, već je načelno određeno da odgovornost snosi onaj tko barata pojedinim procesom i imovinom sukladno djelokrugu posla. Ipak, u Bolnici 1 svaka osoba koja ima pristup medicinskoj dokumentaciji, prije nego što dobije dozvolu za to, mora potpisati Izjavu o povjerljivosti kojom jamči da podatke neće davati trećim osobama. Osobu na mjestu rukovodioca ili službenika za informacijsku sigurnost nema nijedna ustanova, ali je u Bolnici 1 u procesu imenovanje voditelja zbirke osobnih podataka koji će

biti djelomično zadužen za dio te problematike. Međutim, u istoj bolnici primjerice postoji povjerenik za zaštitu podataka iz radnog odnosa, što je također važan aspekt čuvanja informacija. Djelomično postoji i razdvajanje dužnosti, kako nijedan zaposlenik ne bi mogao neovlašteno pristupati ili mijenjati informacijsku imovinu bez odobrenja. To je uglavnom riješeno aplikacijski, *domenskim accountima* koji imaju različite nivoe ovlaštenja, ovisno o opisu posla. Ta hijerarhija osobito je prisutna u Bolničkom informacijskom sustavu (BIS). Primjerice, medicinska sestra s kirurgije može pristupiti samo podacima pacijenata sa svog odjela. Također, ona ima ovlasti unijeti uputnicu, ali je ne može izbrisati. U Bolnici 1 i 3, ako je zaposleniku potreban pristup podacima iz BIS-a van njegovog/njezina odjela, uz pisano obrazloženje, pristup mora zatražiti voditelj odjela. U Bolnici 2 nije dopušten pristup pacijentskim podacima van odjela na kojem osoba radi. Međutim, unatoč jasnim pravilima *igre* i principu *need to know*, prema kojemu zaposlenik ima pristup samo onim podacima koji su mu nužno potrebni, u Bolnici 3 zabilježena je situacija u kojoj su liječnici svoje lozinke za ulaz u BIS davali medicinskim sestrama s kojima rade.

U svim institucijama u kojima se provodilo istraživanje, istaknuto je kako zbog potkapacitiranosti osoblja, osobito informatičke službe, ponekad nisu u mogućnosti razdvojiti osobu koja donosi odluke od one koja je provodi. Ta je razdioba ipak prisutna u segmentu davanja pristupa pojedinim razinama sustava. Primjerice, u Bolnici 1 svaki djelatnik mora ispuniti formular koji se odnosi na njegov opis posla i poziciju, na temelju čega mu administrator daje pojedine nivoe ovlaštenja za segmente u sustavu kojima može pristupiti. Ako zahtjeva pristup BIS-u za podatke van svog odjela, tada od administratora sustava tu dozvolu treba zatražiti voditelj odjela.

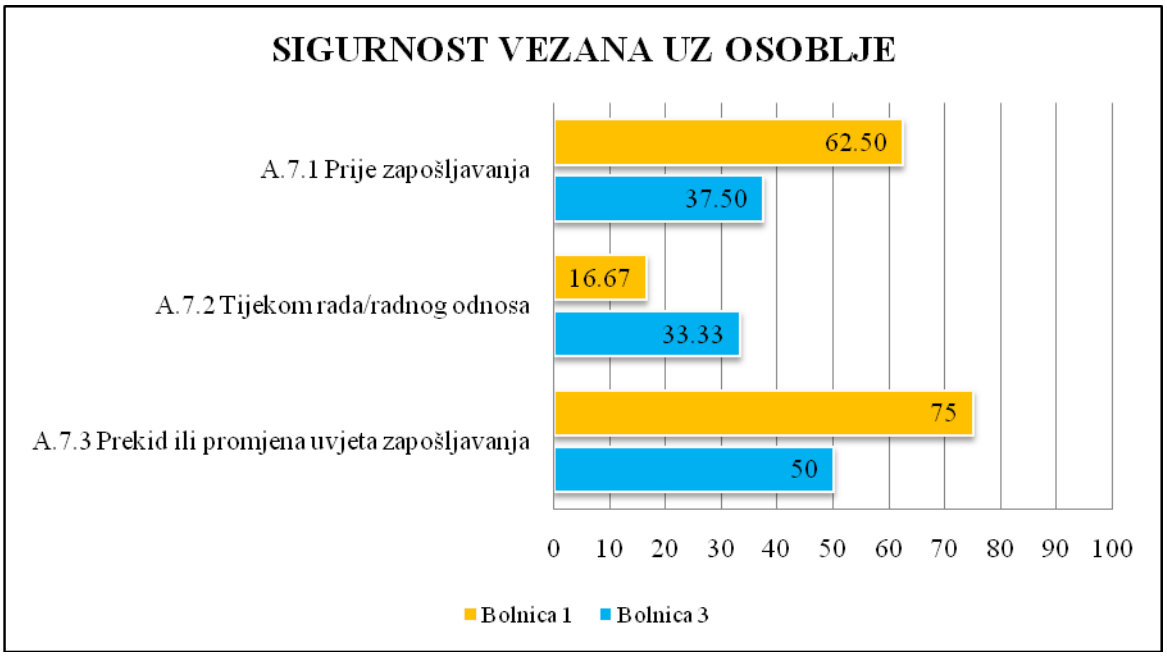
Kada je riječ o kontaktima s ovlaštenim tijelima, kao što su policija, vatrogasci, telekomunikacijske službe, komunalna poduzeća i druge službe, u Bolnici 1 s odgovornim osobama razgovaraju pojedini organizacijski odjeli (primjerice, informatička služba zove telekomunikacijsku tvrtku). Bolnica 3 jedina ima postupnik unutar Odjela zaštite na radu koji definira tko komunicira s drugim službama. U Bolnici 2 pisani ili usmeni postupnik ne postoji već ovlaštena tijela zovu svi po potrebi ili nalogu rukovodioca, odnosno ravnatelja. Ipak, ista bolnica održava najbolje kontakte sa specijaliziranim grupama i forumima iz područja informacijske sigurnosti, kako bi mogli u realnom vremenu razmijeniti informacije o potencijalnim ranjivostima i incidentima, ali i novim načinima zaštite. Druge dvije bolnice te podatke razmjenjuju po potrebi i to međusobno, između nekolicine zdravstvenih ustanova. Sigurnost kao važnu stavku u svim projektima koji se implementiraju unutar bolnice, a nisu

nužno vezani uz informatiku, nema specificiranu nijedna zdravstvena ustanova. Točnije, nije određeno da svi zaposlenici kojima je u opisu posla javljanje na natječaje, pisanje projekata, nabava opreme i slično, moraju u obzir uzeti informacijsku sigurnost, unatoč nastojanjima pojedinih voditelja informatičkih službi da se takva politika implementira u njihovim bolnicama.

Drugi dio poglavlja vezan je uz politiku mobilnih, odnosno, prijenosnih uređaja te rad s udaljenosti. Bolnice su istaknule da u svom svakodnevnom poslu koriste jako malo prijenosnih uređaja te tvrde da zaposlenici na njima ne drže nikakve važne i/li povjerljive podatke jer na njima ne mogu imati instaliran BIS sustav s bolesničkim podacima. Uređaji generalno nisu zaštićeni od krađe i zaposlenike se ne upozorava da ih ne drže na javnim mjestima ili u autu, gdje bi mogli biti na meti neovlaštenih osoba, a sadržaj na njima nije kriptiran. Logički su zaštićeni tek lozinkom za ulaz. Nijedna bolnica nema restrikcije na korištenje privatnih prijenosnih uređaja za potrebe posla, premda ističu da nije učestala praksa da zaposlenici donose svoje uređaje. U Bolnici 3 na privatne laptope instalira se *integrity pristup*, antivirusni softver te im se dodijele resursi s kojima će se spajati. Moguće je i spajanje na bolničku mrežnu infrastrukturu, ali isključivo uz odobrenje administratora mreže. U Bolnici 1 pak zaposlenicima daju uputu da na prijenosnim diskovima ne drže „bolničke stvari“, odnosno informacije vezane uz posao, već ih se savjetuje da sve potrebno za posao imaju na serverima. Kada je riječ o korištenju resursa za obradu informacija u vlasništvu bolnice, osim klasičnog zaduživanja opreme i razduživanja prilikom prekida radnog odnosa, nijedna institucija nema posebna pravila koja bi u obzir uzela ranjivost kućne ili javne mreže te mogućnost da računalu pristupe neautorizirane osobe. Djelomično je to riješeno u Bolnici 3 u kojoj je spajanje preko VPN-a na pojedini poslužitelj zbog rada s udaljenosti, moguće isključivo preko sigurne VPN konekcije, specijalnog softvera i dodijeljenih prava isključivo za vrijeme trajanja određenog projekta.

7.1.3. Usklađenost poglavlja „Sigurnost vezana uz osoblje“ u zdravstvenim ustanovama[20]

Grafikon 3: Rezultati GAP analize za poglavlje „Sigurnost vezana uz osoblje“



Izvor: autorica

ISO standard propisuje i obveznu provjeru kandidata za pojedino radno mjesto, što podrazumijeva provjeru identiteta, verifikaciju potpunosti i točnosti životopisa, priloženih dokumenata o akademskim i drugim kvalifikacijama i eventualne detaljnije provjere, kao što je provjera kriminalističkog dosjea. Kada je riječ o radnom mjestu koje zahtijeva pristup resursima za obradu informacija, ta bi provjera trebala biti još detaljnija. U Bolnici 1, kandidati za posao prilikom prijave i selekcijskog postupka moraju dostaviti presliku dokumentacije propisanu uvjetima natječaja, a prilikom zapošljavanja original ili ovjerene kopije te uvjerenje o nekažnjavanju ne starije od šest mjeseci. Osim zaposlenika, provjeravaju se i volonteri, a za njih se iz sigurnosnih razloga ponekad provjeravaju i izvodi iz prekršajne evidencije. Prilikom intervjua za posao, osoba mora svoj identitet dokazati pokazivanjem osobne iskaznice ili putovnice. Podaci o kandidatima za posao čuvaju se pola godine. Bolnica 3 potvrdu o nekažnjavanju traži tek kod pojedinih radnih mjesta. Informatička pismenost provjerava se kroz desetak teorijskih pitanja i zadatak na računalu kod pojedinih nemedicinskih radnih mjesta. Detaljnije provjere kompetencija koje bi, primjerice, mogli provjeriti u obrazovnoj instituciji koju potencijalni zaposlenik navodi kao referencu u

[20] Iz ovog poglavlja izostala je analiza Bolnice 2 zbog spriječenosti/odsutnosti odgovorne osobe koja je trebala odgovoriti na pitanja koja se tiču sigurnosti vezane uz osoblje.

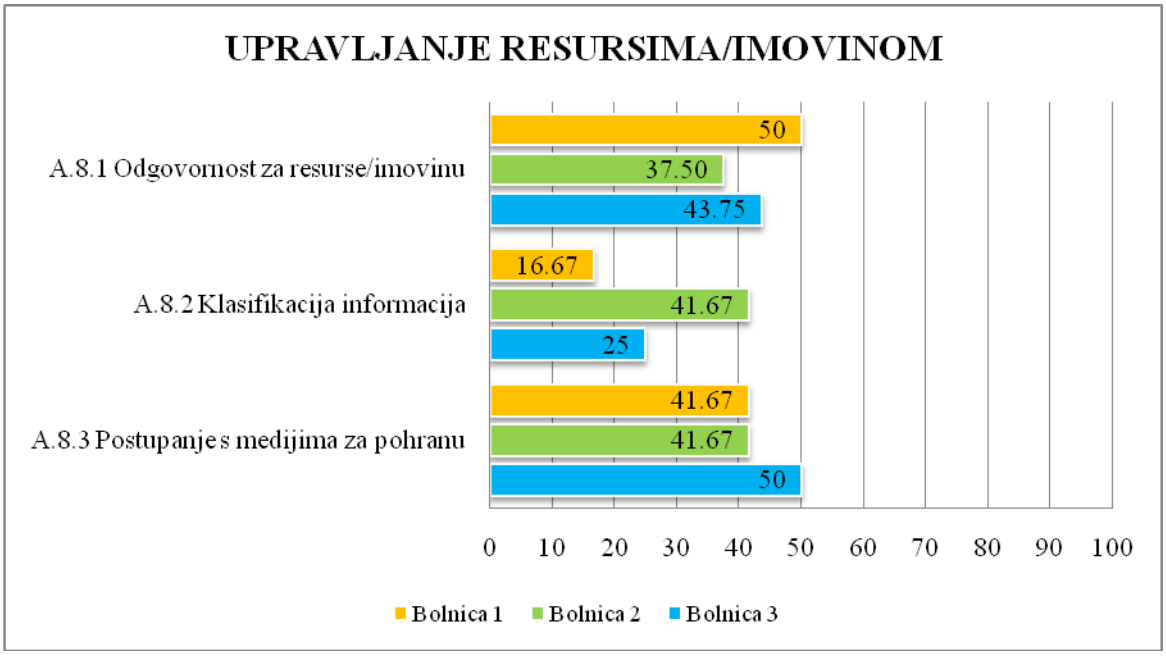
životopisu, u pravilu se ne rade se jer ih odgovorne osobe u bolnicama ne smatraju potrebnim. Prilikom potpisivanja ugovora o radu ili nekog drugog oblika suradnje, svi zaposlenici u Bolnici 1 moraju potpisati o Izjavu o povjerljivosti, dok u Bolnici 3 to nije slučaj. Međutim, posebnih klauzula vezanih uz pitanje informacijske sigurnosti u samim ugovorima o radu nema, a eventualni incident koji bi prouzročili, smatrao bi se općenitom povredom radnih obveza. U Bolnici 3 smatraju da su po tom pitanju prilikom pisanja ugovora bili preblagi te da nije dovoljno da se sankcioniraju samo oni koji izvan bolnice iznesu poslovnu ili profesionalnu tajnu, već i oni koji na benigniji način povrijede informacijsku sigurnost. Međutim, sam disciplinski postupak protiv zaposlenika koji su narušili informacijsku sigurnost ne postoji ni u jednoj bolnici, ako posrijedi nije i jasna povreda radnih obveza. Agencijske radnike nijedna bolnica ne provjerava dodatno, već se oslanjaju na činjenicu da za njih odgovara tvrtka s kojom su potpisali ugovor, ali od njih ne traže dodatnu potvrdu o sigurnosnoj provjeri. Sigurnosni aspekt kod dobavljača ne provjerava ni Bolnica 1 ni Bolnica 3, a u štićenost podataka koje razmjenjuju s njima pouzdaju se odredbama o tajnosti navedenima unutar pojedinog ugovora ili sporazuma.

Kada je riječ o obvezi rukovodstva i odgovornih osoba da zaposlenicima skrenu pažnju na pitanje informacijske sigurnosti i načinima (anonimnog) prijavljivanja incidenata njezinog narušavanja, posebnu praksu za to nemaju ni jedna ni druga bolnica. Prilikom davanja prava pristupa administratori sustava tek dodijele inicijalnu lozinku korisniku i upute ga da ga je promijeni. Predavanja, radionice, učenje na daljinu i drugi načini na koji zaposlenici idu ukorak s informacijskom sigurnošću i razvijaju potrebna znanja i vještine, također su slabo zastupljene. U Bolnici 1 imali su tek nekoliko informativnih predavanja, kako kažu, „po potrebi“. Bolnica 3 edukaciju organizira kad imaju značajne promjene u sustavu, ali zaposlenike ne obvezuju na dolazak. Ipak, optimistično je što planiraju uvesti učenje na daljinu, odnosno web portal na kojem bi zaposlenici kada imaju vremena i oni sami to odluče, odslušali aktualne teme vezane uz informacijsku sigurnost u kontekstu bolničkog sustava te bi na kraju svoje znanje također provjerili malim testom na mreži. Kada postoji potreba za tim, recimo kada se pojave novi oblici prijetnji, u Bolnici 3 svoje djelatnike na opasnost upozoravaju obavijestima na intranetu, u kojoj ih upućuju da ne otvaraju sumnjive e-mailove ili ne skidaju priloge, već ih automatski brišu. Važnost ljudskog faktora u informacijskoj sigurnosti ili pak njezinom narušavanju osobito je izražena u Bolnici 3. U njoj su, u nekoliko navrata, zbog posjete nepoćudnim stranicama koje su na računalo „zakačile“ zlonamjerni softver, morali upozoravati djelatnike na štetu koju nanose instituciji, a u jednom

ih je slučaju praćenje transakcijskih logova dovelo i do informacija o pronevjeri. To je još jedna potvrda argumenta da niti uz sav mogući softver i tehničke alate nije moguće prevenirati ranjivost ako postoji osoblje s nepoćudnim i zlonamjernim motivima ili pak ono nedovoljno informacijski/informatički upućeno. Nakon prestanka zaposlenja, u Bolnici 1 tvrde da se korisnički račun bivših zaposlenika automatski briše te da se na mjesečnoj bazi radi izvještaj o tome. Izjava o povjerljivosti i bivše zaposlenike u Bolnici 1 trajno obvezuje da čuvaju osjetljive podatke o bolnici i svim aspektima s kojima se susrela tijekom rada, dok u Bolnici 3 navode da su u ugovoru o radu propustili obvezati bivše zaposlenike na čuvanje poslovne tajne. Ukoliko otkaz o radu ne nastupi sporazumno već je rezultat povrede radnih obveza ili inicijativa poslodavca, nijedna bolnica nema mehanizme kojima bi dodatno kontrolirala kopira li potencijalno gnjevni zaposlenik pojedine osjetljive podatke o bolnici koje bi je mogle kompromitirati.

7.1.4. Usklađenost poglavlja „Upravljanje resursima/imovinom“ u zdravstvenim ustanovama

Grafikon 4: Rezultati GAP analize za poglavlje „Upravljanje resursima/imovinom“



Izvor: autorica

U sve tri bolnice postoji inventarna lista s popisom resursa i imovine za obradu informacija koja se provjerava jednom godišnje. U Bolnici 1 popisuje se fizička oprema (hardver), dok se za softversku (aplikacijski i sistemski softveri, baze podataka) i

informacijsku imovinu (podaci u bazama, programski kodovi, korisnički priručnici) podrazumijeva da je na računalu, ali ne postoji popis imovine kao takav. Odgovorna je osoba koja se nalazi na inventarnoj listi, a ako se oprema premjesti, dužna je o tome obavijestiti osobu zaduženu za inventar. U Bolnici 2 radi se popis jedino hardverske imovine, inventarnu listu supotpisuje ravnatelj, a za opremu je odgovoran odjel ili osoba koja ju je naručila. Bolnica 3 ima popis hardverske i informacijske imovine, ali nema popis svih baza podataka. Informacijska imovina i pojedini kodovi za pristup mrežnoj opremi čuvaju se u zatvorenoj kuverti u ormaru pod ključem koji ima voditelj informatičke službe. Inventarne liste za fizičku opremu sadrže podatke o tome gdje i kod koga se imovina nalazi, kada je nabavljena i slično. Vlasnici imovine, ne u pravnom smislu, već onom praktičnom, kao osobe koje su zadužene za sigurnost i brigu o pojedinoj imovini nisu posebno imenovani, kao niti njihova zaduženja. U Bolnici 3 se, primjerice, odgovornom osobom za pojedinu imovinu smatra glavna sestra nekog odjela, ali ni u kojem pravilniku to nije specificirano. Kada je riječ o pravilima za prihvatljivo korištenje informacijske imovine, u Bolnici 2 drže se naputaka Carneta i proizvođača opreme, ali ne postoje interni pravilnici o tome, osim politike korištenja službenih e-mailova.

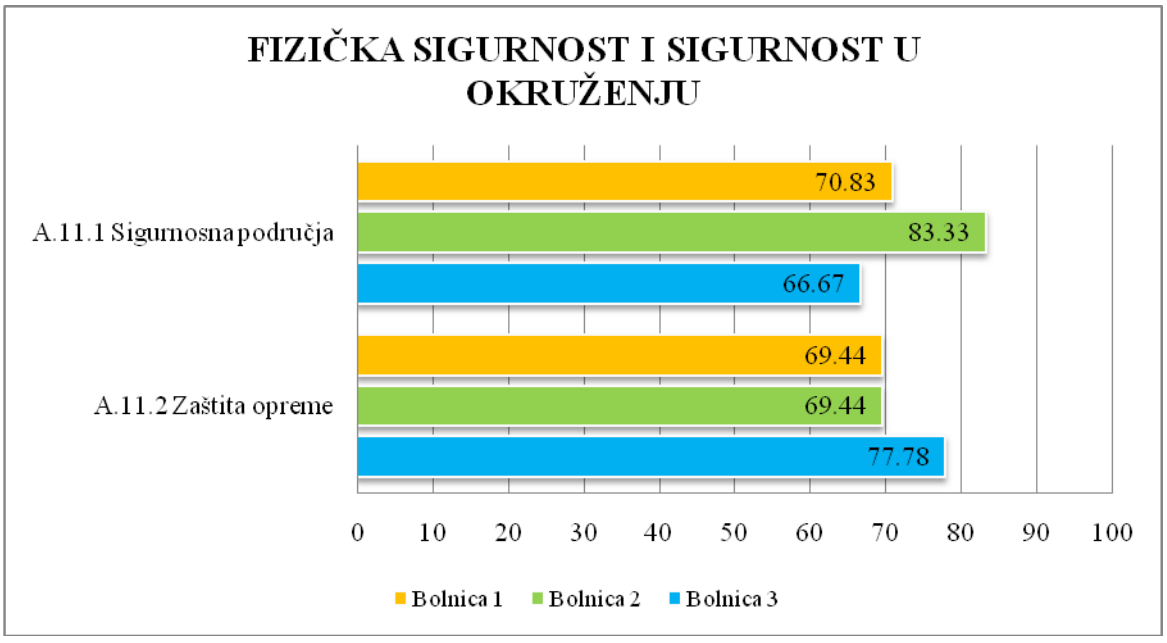
Dakako, u svim je bolnicama pravilo da se osoba nakon prestanka radnog odnosa, mora razdužiti za sve što je koristila, pa tako i informacijsku opremu, ali se ne provjeravaju USB-ovi i diskovi na koje je bivši zaposlenik mogao spremiti podatke jer bolnice generalno smatraju da povjerljive podatke čuvaju samo na serverima. U Bolnici 1 brišu sve podatke i korisničke račune s domenskog servera, dok u Bolnici 3 tek privremeno suspendiraju račune.

Kada je riječ o klasifikaciji informacija, takav postupnik postoji jedino u Bolnici 2, u kojoj je na snazi Pravilnik o tajnosti koji precizira što se smatra kojom vrstom tajnog podatka. Sukladno tome postoje tri stupnja klasifikacije te su predviđene sankcije za povredu Pravilnika. Međutim, takva politika klasifikacije u pismenom obliku datira još iz 2000-ih te, s obzirom na tehnološke promjene i promjene u poslovanju, nikada nije revidirana ili izmijenjena. Do određene razine u sve tri bolnice riješena je politika postupanja s informacijskom opremom te su se bolnice osigurale da postoji, primjerice, evidencija o tome tko, što i zašto briše iz BIS-a, kao sustava u kojem su najosjetljivije vrste podataka, oni vezani uz pacijente i povijesti bolesti. Međutim, ono što su u Bolnici 3 istaknuli kao problem jesu pojedini zahtjevi HZZO-a za slanje popisa liječnika starijih od 60 godina e-mailom, kao običan prilog, bez šifriranja, što je potencijalna opasnost jer se u istom dokumentu šalju i OIB i drugi osobni podaci.

Što se tiče upravljanja prijenosnim medijima, ne vodi se pretjerano računa o tome da je sadržaj na takvim medijima kriptiran, da se traži dozvola za iznošenje opreme van bolnice i slično. U Bolnici 3 postoji *checkpoint integrity*, odnosno softver koji evidentira sve što se snima na USB. Kada se rashoduju diskovi i drugi prijenosni mediji, za slučaj da se na njima nalaze povjerljivi podaci, u Bolnici 1 i Bolnici 3 s njih se prvo bespovratno brišu svi podaci, a onda se i fizički trgaju i uništavaju, nakon čega se šalju na elektronski otpad. Kod fizičkog prijenosa medija i informacija, u Bolnici 1 moguće je da se zatraži uvid u medicinsku dokumentaciju koji se onda pacijentima šalje običnom poštom, ali prije toga u bolnicu moraju dostaviti pisani zahtjev i presliku osobne iskaznice i rodnog lista. Također, fizički se prenose i CD-i s fakturama koje se dostavljaju HZZO-u. Jedina je zaštita što te medije ne prevozi dostavna služba već zaposlenik bolnice, ali je zabrinjavajuća činjenica da sadržaj nije kriptiran već samo potpisan s dva certifikata FINA-e koji garantiraju jedino da sadržaj nije mijenjan.

7.1.5. Usklađenost poglavlja „Fizička sigurnost i sigurnost u okruženju“ u zdravstvenim ustanovama

Grafikon 5: Rezultati GAP analize za poglavlje „Fizička sigurnost i sigurnost u okruženju“



Izvor: autorica

Sukladno zakonskim osnovama koje moraju ispunjavati po pitanju fizičke sigurnosti, sve su bolnice, koliko je to moguće, adekvatno osigurane od vanjskih prijetnji, kao što su

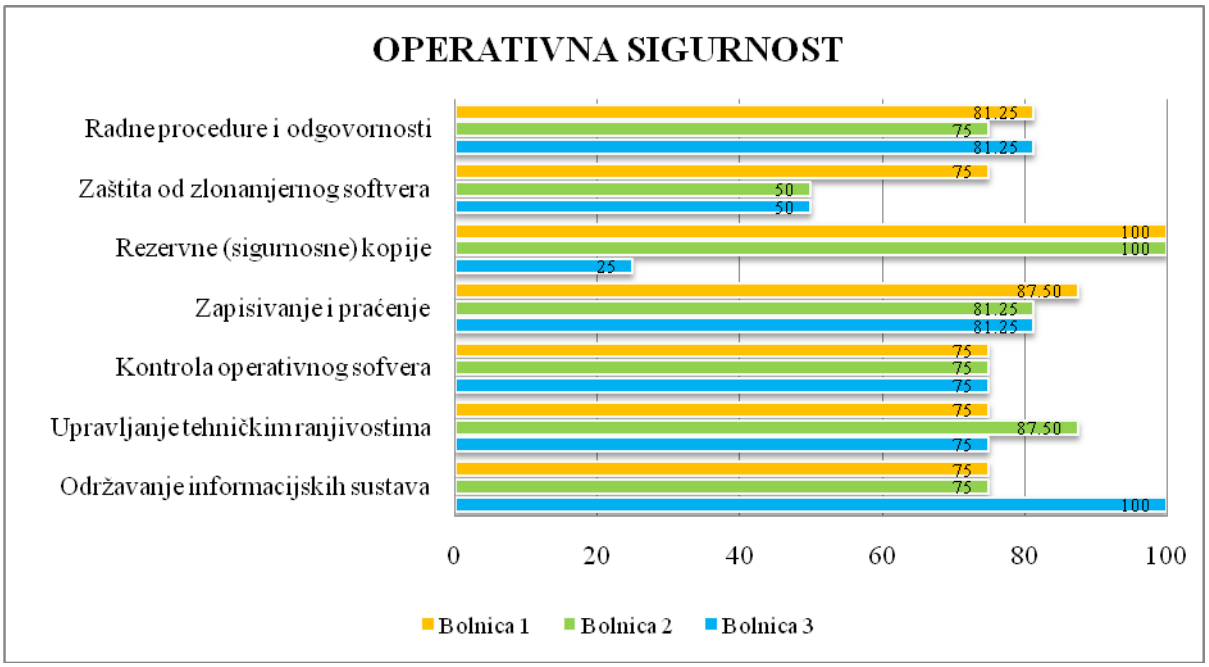
poplave, potresi i druge nepogode. Odjel zaštite na radu i zaštite od požara vodi računa o tome da se u redovnim vremenskim intervalima ispituju ventilacija, klimatizacija i ostali sustavi važni za funkcioniranje ustanove. Sve bolnice imaju neprekidne izvore napajanja, odnosno UPS-ove i agregate te zasebne trafostanice, a razvodne su kutije pod ključem. Mrežna infrastruktura odvojena je od telefonske te 24 sata na dan postoje dežurni električari i vatrogasci. Uredi i ostale prostorije zaključavaju se, a u bolnicama i krugu njihovih dvorišta postoji videonadzor. Premda politika bolnice nalaže zaključavanje svih ureda i prostorija, u Bolnici 3 ta praksa nije najbolje usvojena, osobito nakon radnog vremena, kada spremačice čiste urede uprave, pa se nerijetko događa da su 45 minuta od kraja radnog vremena, te prostorije i dalje otključane.

Sigurnosna područja u kontekstu informacijskih resursa, kao što su server soba i fizička arhiva medicinske dokumentacije, u svim su bolnicama dodatno kontrolirana i nalaze se u protupožarnim zonama. Pravo na pristup server sobi ima tek nekoliko djelatnika iz informatičke službe, a ako pristup njoj trebaju djelatnici iz vanjskih tvrtki koje održavaju pojedini dio sustava, moraju biti u prisustvu voditelja informatičke službe. Međutim, detaljniji podaci o ulasku u server sobe, kao što su vrijeme ulaska, podaci o osobama koje su ušle i slično, niti u jednoj bolnici ne evidentiraju se. Bolnica 2 prostor server sobe planira kontrolirati i kamerama. Server sobe fizički su zaštićene protuprovalnim vratima s ključevima, a u slučaju Bolnice 2, riječ je o posebno kodiranim ključevima s rupicama koji se ne daju kopirati. Pristup arhivi zaštićen je ključem i čuva ga arhivistica koja zapisuje ako netko od liječnika iznosi medicinsku dokumentaciju van.

Drugi dio poglavlja vezan je uz nenadgledanu korisničku opremu te politike praznog stola i ekrana kojima se savjetuje da se osjetljivi podaci, kao što su, konkretno, bolesničke povijesti bolesti u papirnatom obliku, ne ostavljaju na stolu bez nadzora i da se odmah uklone iz printera. Politika praznog ekrana nalaže da se računalo zaključava i štiti lozinkom za ulaz kada se ne koristi. U svim je bolnicama to riješeno automatskom odjavom i gašenjem nakon 10-30 minuta. Međutim, Bolnica 3 navodi da upozoravaju svoje zaposlenike da i sami prilikom izlaska iz prostorije zaključavaju računala, ali ističu kako se oni toga slabo pridržavaju, baš kao i u slučaju Bolnice 2, gdje postoji problem s ostavljanjem medicinske dokumentacije po stolovima bez nadzora.

7.1.6. Usklađenost poglavlja „Operativna sigurnost“ u zdravstvenim ustanovama

Grafikon 6: Rezultati GAP analize za poglavlje „Operativna sigurnost“



Izvor: autorica

Poglavlje vezano uz radnu sigurnost, odnosno sigurnost radnih operacija uglavnom je vezano uz zadovoljavanje informatičkih kontrola, kao što su održavanje informacijskih sustava, zaštita od zlonamjernog softvera, upravljanje tehničkim ranjivostima, zapisivanje rada na sustavu u logovima, instaliranje zakrpa, ažuriranje operativnog softvera, ograničenja u pogledu instalacije softvera, izrade rezervnih kopija informacija i slično.

Ono što je zajedničko svim bolnicama jest da su ograničile instalaciju softvera tako da obični korisnici bez administratorskih ovlasti ne mogu ništa instalirati na računalo. Kao efikasan mehanizam zaštite od zlonamjernih softvera, voditelji informatičkih službi u bolnicama istaknuli su upravo različite nivoe ovlaštenja koji korisnicima standardnih domenskih računa ne daju previše prostora za manipulaciju. S tehničke strane, riješeno je da sve bolnice imaju različite antivirusne programe licenciranih proizvođača, a u slučaju Bolnice 3 i *antimalware* programe. Iste programe ima i Bolnica 1, koja uz to koristi i *spy hunter* program. Međutim, u slučaju Bolnice 1 i Bolnice 3 koje na dosta računala još uvijek koriste zastarjeli Windows XP, pojedini proizvođači antivirusnog softvera upozorili su ih da bez nadogradnje ne mogu jamčiti stopostotnu sigurnost. Dodatni je problem što Bolnica 1 uz to koristi i nelicencirane verzije operativnog sustava. Crne liste internetskih stranica koje upozoravaju i blokiraju korištenje sumnjivih adresa koriste Bolnica 2 i djelomično Bolnica 3.

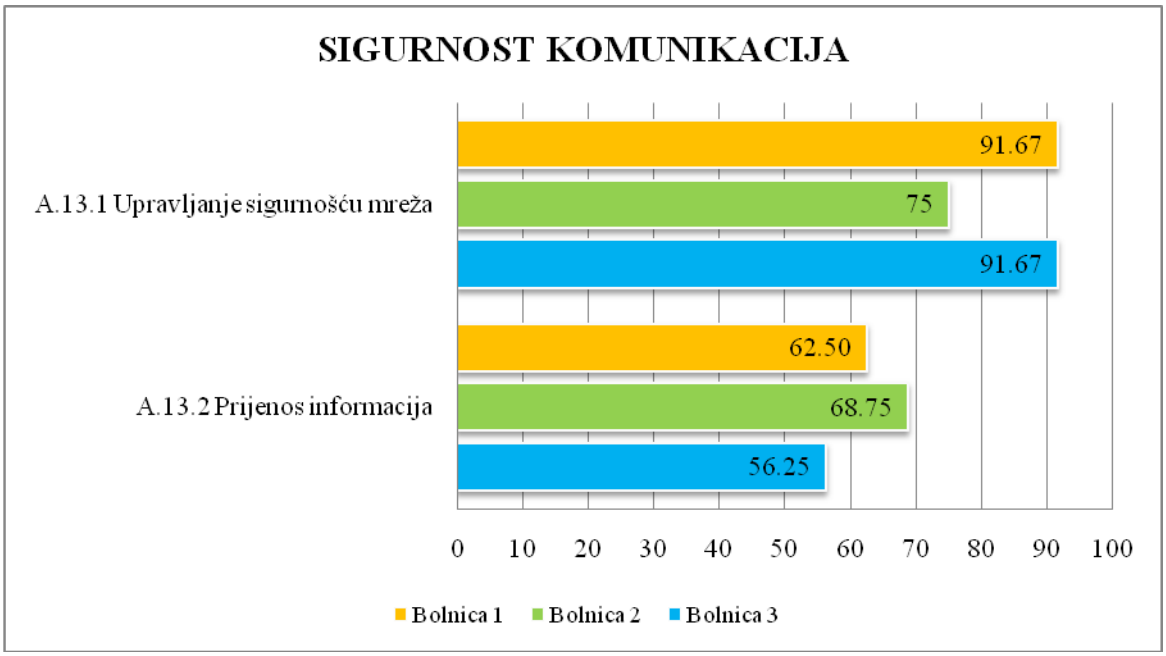
Aktualne se liste preuzimaju i postavljaju na vatrozidu, a posebna se filtriranja dodaju prema potrebi ili dojavi, kada je riječ o Bolnici 2. Sustav koji bilježi takve stranice imala je i Bolnica 3, ali otkako su upali u financijske probleme, otkazali su licencu te program jedino bilježi što se događa na mreži, ali ne zabranjuje, tj. ne blokira ulaz na takve stranice. U toj zdravstvenoj ustanovi kao velik problem ističu nedostatak financijskih sredstava za sigurnost te su svjesni da bi trebali nadograditi sigurnosti sustav jer nije *up to date*.

Sve bolnice prije puštanja pojedine aplikacije u rad, testiraju je u posebnom, testnom okruženju koje je odvojeno od produkcijskog, kako ne bi omelo rad korisnika ili poremetilo rad sustava. Logovi koji bilježe sve aktivnosti korisnika u Bolnicama 1 i 2 pregledavaju se po potrebi, ukoliko nešto upućuje na nepravilnosti, dok se uz tu mjeru, u Bolnici 3 logovi pregledavaju i periodično, neovisno o tome sumnja li se na incident narušavanja informacijske sigurnosti ili ne. Kako ne bi došlo do zloupotrebe, pohranjuju se i administratorski dnevnici logova.

Možda najvažnije pitanje operativne sigurnosti je i backup, odnosno rezervna kopija informacija. U svim bolnicama postoji backup podataka na magnetne trake, a u Bolnici 1 i 2 i na različite servere. Radi se backup svih baza podataka, mailboxa, bolničkih podataka, intranet stranica.. Baze s pacijentskim podacima čuvaju se trajno te su u slučaju Bolnice 1 i 2 kriptirane te se rade u realnom vremenu. Također, u tim zdravstvenim ustanovama rezervne kopije podataka čuvaju se u dvije različite zgrade, odnosno, dislocirane su i to u prostorijama koje imaju alarm za temperaturu, vlagu i vibraciju te protuprovalna vrata, a u slučaju Bolnice 2, u klimatiziranim poslužiteljskim prostorima s kodiranim ključevima te u sefu prema postupcima zaštite materijala u sefu. Bolnica 1 jedina ima i dodatni server koji služi kao *disaster recovery* na koji se mogu prebaciti podaci u slučaju kriznih situacija i koji onda može poslužiti kao produkcijski server. Najveći problem ima Bolnica 3 koja terminal za *robotski* backup podataka ima u server sobi. Prema ISO standardima, ali i pojedinim zakonskim preporukama, rezervne kopije informacija moraju se čuvati na udaljenom mjestu, dislocirane, tako da u slučaju požara, krađe ili drugih situacija koje dovode do uništenja podataka u kriznim situacijama, ti podaci ne nestanu nepovratno. Sličan je problem prije nekog vremena i promjene sigurnosne paradigme imala i Bolnica 1 koja je backup podataka imala na istom serveru koji koriste za svakodnevni rad. Zbog toga su dva tjedna bili bez servera, ali i podataka jer je zlonamjerni softver, točnije kriptoloker napao nekoliko računala i server te zaključao bazu podataka. Podatke su na kraju uspjeli vratiti, ali su ih taj incident i oporavak, osim živaca, koštali i podosta financijskih sredstava.

7.1.7. Usklađenost poglavlja „Sigurnost komunikacija“ u zdravstvenim ustanovama

Grafikon 7: Rezultati GAP analize za poglavlje „Sigurnost komunikacija“



Izvor: autorica

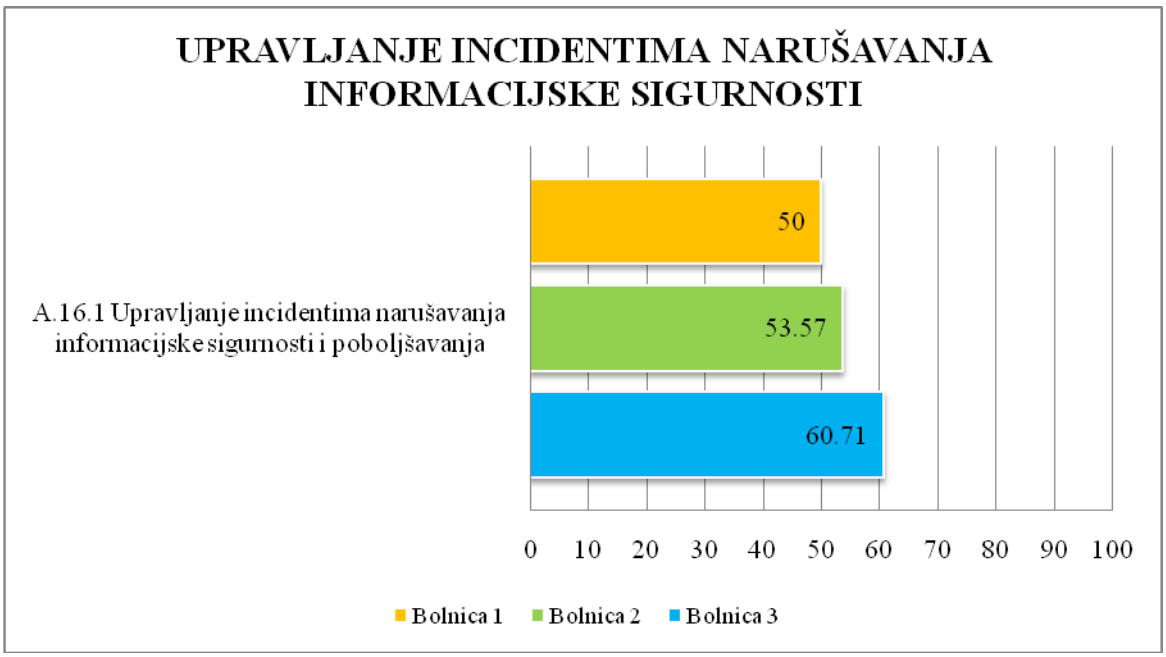
Kontrole vezane uz sigurnost komunikacija definiraju upravljanje mrežama, sigurnost mrežnih usluga, razdvojenost mrežnih domena te politike razmjene elektronskih poruka.

Kada je riječ o sigurnosti mreže, sve zdravstvene ustanove koje su sudjelovale u istraživanju adekvatno su riješile pitanje mrežne sigurnosti. Primjerice, u Bolnici 1 postoje dvije mreže, jedna za goste, odnosno, pacijente, a druga za osoblje. One su na zasebnim VLAN-ovima tako da nema nikakve šanse da se pacijenti spoje na bolničku domenu niti dođu do servera za produkciju. Postoje različiti načini zaštite, odnosno tehnologije za autentifikaciju, enkripciju i kontrolu pristupa mreži te korištenje https protokola.

Kada je riječ o prijenosu informacija, ne postoje točno određene politike o korištenju i razmjeni poruka preko mreže, ali ono čime se primjerice štiti Bolnica 2 je za potpisana Pristupnica za autentikacijski i autorizacijski AAI@Edu identitet kojom se jamči da će se pridržavati Carnetovih pravila o sigurnosti na mreži. Također, Bolnica 3 neko vrijeme koristila je filtriranje lista web stranica te je bilo onemogućeno korištenje društvenih mreža, internet kladionica i slično.

7.1.8. Usklađenost poglavlja „Upravljanje incidentima narušavanja informacijske sigurnosti“ u zdravstvenim ustanovama

Grafikon 8: Rezultati GAP analize za poglavlje „Upravljanje incidentima narušavanja informacijske sigurnosti“



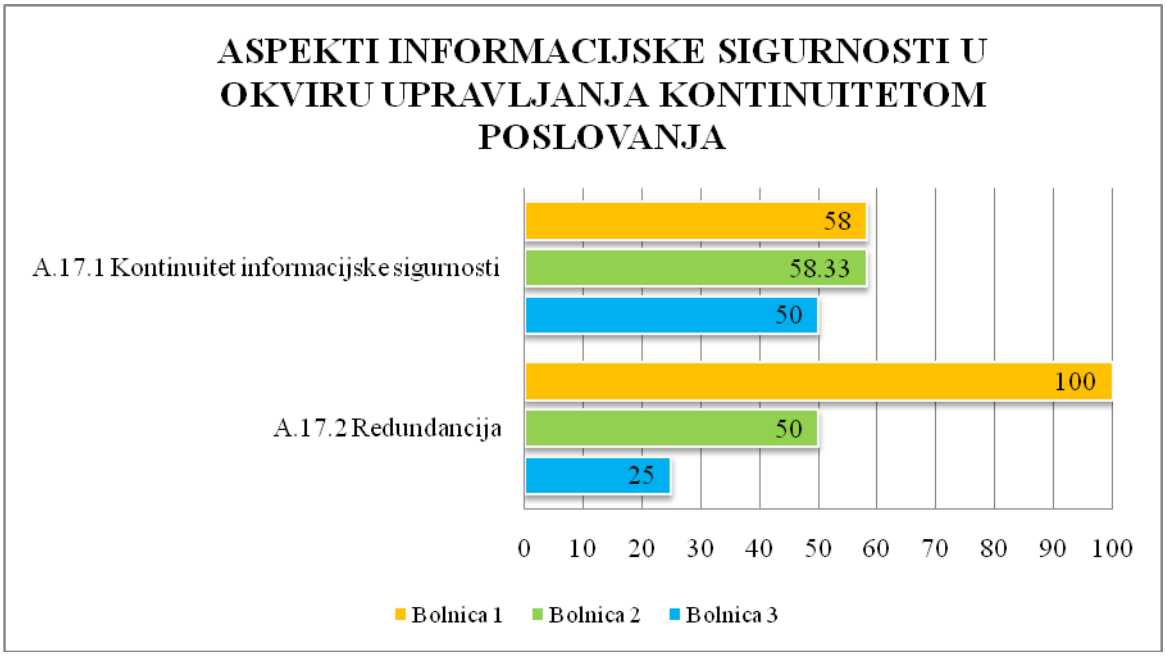
Izvor: autorica

U slučaju incidenta narušavanja informacijske sigurnosti, bilo da je riječ o unutarnjem ili vanjskom upadu, u Bolnici 2 utvrđuje se izvor, moguća odgovornost te se obavještava poslovodstvo, dok u Bolnici 1 nisu precizno utvrđene uloge i odgovornosti tehničkog osoblja i drugih zaposlenika u toj situaciji. Slična je situacija i u Bolnici 3, a svim zdravstvenim ustanovama zajedničko je da ne vode evidenciju o (potencijalnim) ranjivostima i incidentima. U svim bolnicama ukoliko dođe do upada u sustav, nastoji se otkriti odakle je prijetnja stigla, koji je doseg zaraze zlonamjernim softverom te se pristupa otklanjanju posljedica incidenata. Ako je utvrđena osobna odgovornost nekog od zaposlenika, to se prijavljuje rukovodstvu. Bolnica 1 prije godinu dana imala je slučaj zaraze nekoliko računala kriptolokerom, a Bolnica 2 godišnje bilježi 10-15 slučajeva narušavanja informacijske sigurnosti. Kada je riječ o Bolnici 3, ove godine nisu zabilježili proboj, ali su zato prošle godine imali dva veća incidenta u kojima je došlo do proboja iz jedne organizacijske jedinice u drugu kroz dijeljene resurse. Konkretno, zaposlenik Odjela zaštite na radu na pornografskim stranicama pokupio je virus kojim je zarazio ne samo lokalno računalo, već i mrežni disk jer za potrebe posla, taj Odjel ima određeni pristup dijelu kadrovske evidencije. Zaposlenici su odmah primijetili da se nešto događa i da nešto nije u redu s dokumentima te su događaj prijavili informatičkoj

službi koja je krenula u čišćenje virusa. Bolnica 1 i 2 dosad nisu susrele s incidentima u koje bi se trebala uključiti i nadležna tijela sustava, kao što su policija, tužiteljstvo ili sud te su odgovorne osobe u Bolnici 1 dodatno navele kako u smislu forenzike ne prikupljaju moguće dokaze niti imaju razrađenu proceduru. Za razliku od njih, Bolnica 3 ponekad provodi vlastite istražne radnje te su tako otkrili slučaj pronevjere na blagajni. Kroz transakcijske logove na poslovnom sustavu dokazivali su da je nastupilo kazneno djelo. Te su dokaze predali tužiteljstvu koje nije naložilo da se logovi isključe, odnosno, izdvoje iz regularne arhive kako bi bili trajno dostupni za eventualne potrebe sudskog procesa, što govori o slaboj razini poznavanja novih oblika kaznenih djela vezanih uz informacijske sustave. Također, prema naputku iz ISO standarda, u takav bi se proces već na početku trebala savjetodavno uključiti i pravna služba pojedine tvrtke/institucije, što u Bolnici 3 nije bio slučaj upravo zbog nepoznavanja pravnih i istražnih procesa vezanih uz ovu problematiku.

7.1.9. Usklađenost poglavlja „Aspekti informacijske sigurnosti u okviru upravljanja kontinuitetom poslovanja“ u zdravstvenim ustanovama

Grafikon 9: Rezultati GAP analize za poglavlje „Aspekti informacijske sigurnosti u okviru upravljanja kontinuitetom poslovanja“



Izvor: autorica

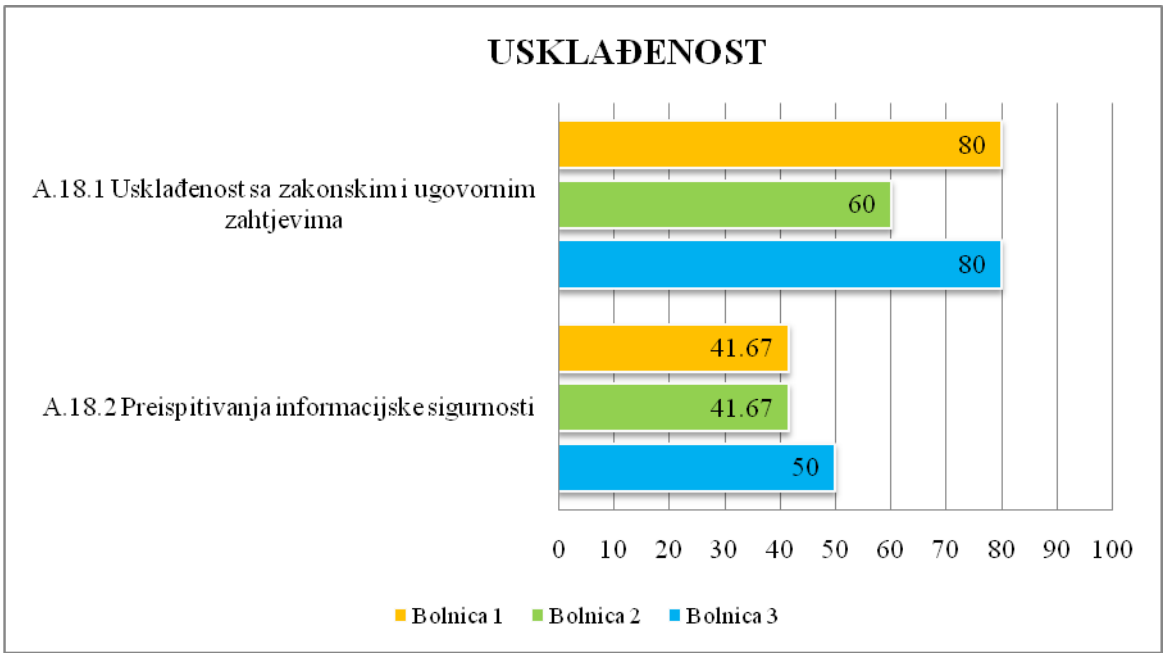
Nepisano je pravilo da u svakoj bolnici postoji određeni krizni tim za upravljanje oporavkom od katastrofa u slučaju događaja koji bi posredno ili neposredno utjecao na

informacijsku sigurnost. Međutim, detaljno razrađeni i dokumentirani planovi mogućih scenarija katastrofa ili kriza te odgovora na njih ne postoje.

Kada je riječ o redundantnosti, odnosno sekundarnom mjestu IT infrastrukture koja bi se mogla iskoristiti u slučaju krize ili katastrofe, kompletan *disaster recovery server* ima tek Bolnica 1. Taj server nema veze niti s testnim niti produkcijskim serverom već on preuzima na sebe produkciju cijelog sustava ako svi ostali serveri „puknu“ te osigurava da se i u kriznim uvjetima rad normalno nastavlja. U Bolnici 2 postoji redundancija na razini lokalne IT opreme, ali ne i kompletnog data centra. Sekundarno mjesto u slučaju krize ili katastrofe nema Bolnica 3 zbog nedostatka financijskih sredstava. Kako ističu, unatoč tome što prate trendove u informacijskoj sigurnosti i pokušavaju primijeniti moderna tehnološka rješenja, ako nema novca za tu namjenu, iluzionarno je razgovarati o realnom upravljanju kontinuitetom poslovanja.

7.1.10. Usklađenost poglavlja „Usklađenost“ (s pravnim zahtjevima) u zdravstvenim ustanovama

Grafikon 10: Rezultati GAP analize za poglavlje „Usklađenost“



Izvor: autorica

Sve su bolnice zakonski usklađene sa Zakonom o zaštiti osobnih podataka, dok se po pitanju prava intelektualnog vlasništva Bolnica 2 nalazi u „sivoj“ zoni jer koristi nelicencirane softvere. Reviziju informacijskih sustava u Bolnici 1 i 2 vrše stručnjaci iz

CERT-a i CARNET-a, dok u Bolnici 3 ponekad angažiraju i komercijalne tvrtke kao konzultante. Unutar te zdravstvene ustanove postoji i ideja o certificiranju po ISO standardima informacijske sigurnosti.

7.2. Energetska kompanija

Energetska tvrtka koja je sudjelovala u istraživanju ima provedene gotovo sve kontrole propisane ISO/IEC 27001:2013 standardu. Premda spomenuti standard nemaju implementiran, odnosno nemaju certifikat o njegovoj primjeni, svoje svakodnevno poslovanje uskladili su prema njemu. Tako, osim generalne, krovne politike informacijske sigurnosti koja je dostupna svim zaposlenicima na intranetu, imaju implementirane i niže politike koje detaljno reguliraju kontrolu pristupa, fizičku sigurnost, upravljanje sigurnosnim incidentima i slično. Definirani su i vlasnici imovine te su razdvojene dužnosti između osoba koje donose odluke, onih koji ih provode i onih koji su kao rukovodioci za njih odgovorni. Na godišnjoj razini provode svoj interni audit i po potrebi revidiraju politiku informacijske sigurnosti. Ono u čemu se razlikuju od zdravstvenih ustanova jest i činjenica da je sigurnost implementirana u svaki njihov projekt, a ako generalne odredbe o informacijskoj sigurnosti osoba koja piše i razvija projekt nije implementirala već u ranim fazama, stručnjaci za sigurnost projekt joj vraćaju na doradu. S tehničke strane, riješeni su svi preduvjeti za informacijsku sigurnost, kao što su kontrole protiv zlonamjernih softvera, crne liste stranica na koje se pale alarmi, mrežne domene...

Postoji i detaljno razrađena politika korištenja prijenosnih uređaja pa tako informacijska oprema uvijek mora biti uz osobu i ne smije se ostavljati na javnom mjestu bez nadzora. Ako se računalo ostavlja u automobilu, mora se spremiti u prtljažnik, a prije toga zaključati posebnom sajlom za laptop. Privatna prijenosna računala za potrebe posla nisu dozvoljena i ne omogućuje se mrežni pristup na njima. Svi zaposlenici moraju svake dvije godine proći testiranje vezano uz informacijsku sigurnost nakon završene edukacije o načinu upravljanja s prijenosnim uređajima, korištenju lozinki i slično. Testiranje se provodi u praktičnom okruženju, preko web obrasca. Čak i osobe koje se u svom radu neposredno ne dotiču uređaja za obradu informacija moraju ispuniti test u pisanoj formi. Kada je riječ o korištenju prijenosne opreme, zaposlenicima se daju USB-ovi s pinovima, odnosno kriptiranim sadržajem. Postoji i Pravilnik o klasifikaciji dokumenata koji prati zakonsku shemu klasifikacije, a koji se primjenjuje ovisno o financijskim, operativnim i poslovnim rizicima. Na svim dokumentima stupanj povjerljivosti označen je u gornjem desnom kutu,

kao i broj dokumenta koji je naveden u registru. Važni dokumenti uređuju se i čuvaju u zajedničkom *cloudu* (virtualnom podatkovnom centru) te postoji nekoliko mapa sa sadržajem, ovisno o razini pristupa. Svako otvaranje, brisanje ili promjena pojedinog dokumenta bilježi se i kontrolira je stručnjak za informacijsku sigurnost. Data centri prikladno su zaštićeni kamerama, protuprovalnim i protupožarnim vratima, a na ulazu u objekt nalazi se i čuvar. Svakih mjesec dana, neovisno o tome je li došlo do promjena ili ne, radi se popis osoba koje imaju ovlast ući u data centar.

Za gotovo svaki dio politike informacijske sigurnosti koju propisuje ISO standard postoji mali odjel koji brine o pojedinom segmentu. Razrađenost politika u pojedinim je slučajevima toliko detaljno razrađena da zaposlenicima u opisu posla stoji da moraju kontrolirati jedni druge, odnosno, provjeravati zaključavaju li njihovi kolege urede, gase li računala i brinu li generalno o *praznim stolovima i ekranima*.

8. ZAKLJUČAK

„Sruši“ li se zdravstveni sustav samo jedne bolnice, na kojem se nalaze duboko privatni podaci tisuće pacijenata, nacionalna sigurnost bila bi neminovno ugrožena. A da je zdravstveni sustav jedan od najranjivijih dijelova kritične infrastrukture, pokazao je i nedavni napad kriptolokerom vrlo simboličnog naziva WannaCry. Pukom srećom što je Hrvatska kao takva još uvijek nedovoljno zanimljiva meta kriminalcima „izvana“, izbjegle su se posljedice s kakvima su se suočile engleske bolnice. S obzirom na stanje informacijske sigurnosti u bolnicama obuhvaćenim istraživanjem, stanje nije optimistično i postoji realna bojazan o ranjivosti tih institucija koja se već u nekoliko navrata ispostavila točnom. Sa zlonamjernim softverima i probojima sve su se tri bolnice zasad uspješno suočile, ali činjenica je da se tehnologija i vještine nepoćudnih kriminalaca novog doba svakodnevno sve više razvijaju i upitno je do kada će se zdravstveni sustavi moći odupirati tim prijetnjama. Pogotovo sa zastarjelim, ponegdje i nelicenciranim softverima i Windows XP operativnim sustavima bez mogućnosti nadogradnje te držanjem rezervnih kopija podataka u server sobi koju samo jedna veća katastrofa poput potresa može odnijeti.

Stanje informacijske sigurnosti u zdravstvenim ustanovama obuhvaćenim istraživanjem, generalno gledano, daleko je od idealnog. Za razliku od njih, analizirana energetska tvrtka pitanje sigurnosti riješila je na dobar način – vodeći se dobrom praksom i implementirajući kontrole iz međunarodno prihvaćenih standarda. U bolnicama prvenstveno nedostaje sistematičnosti, te nedostaje čitav niz politika i pravilnika koji bi regulirali pitanje informacijske sigurnosti, a što je nužno za izgradnju sigurnog i cjelovitog sustava upravljanja. Kao što je već navedeno, glavni su problemi vezani uz nedostatak sredstava, ali i izostanak svijesti zaposlenika i (ne)medicinskog osoblja o važnosti (mjera) cyber sigurnosti.

Zbog toga bi, u smislu kratkoročnih mjera, bilo dobro pokrenuti program edukacije i osvješćivanja osoblja o pitanjima informacijske sigurnosti. Nije za očekivati da svi zaposlenici postanu informacijski eksperti, ali važno im je skrenuti pažnju na ranjivosti kojima je cijeli sustav okružen, a koje, barem djelomično oni mogu prevenirati svojim savjesnim postupanjem. Da je upravo ljudski, a ne tehnički faktor izazvao nekoliko proboja, potvrđeno je i rezultatima analize u jednoj bolnici, a to, sudeći po svemu viđenom, vjerojatno nije izolirani slučaj. Dobro bi bilo i imenovati osobu odgovornu za informacijsku sigurnost, ali ne u smislu dodavanja te funkcije voditelju informatičke službe, već angažiranjem neovisne osobe van tog sustava. Ta bi osoba osim za trendove u informacijskoj sigurnosti i

popisivanje nedostataka mogla biti zadužena i za pronalazak raspisanih natječaja za dodjelu financijskih sredstava iz europskih fondova, kojima bi se mogao povući novac za sigurnost.

Dugoročno gledano, trebao bi se poboljšati sustav upravljanja incidentima narušavanja informacijske sigurnosti te bi trebao postojati plan oporavka i funkcioniranje u kriznim situacijama. Ne bi bilo loše uz to napraviti i procjenu rizika, kako bi se ustanovilo koje su slabosti i potencijalni nedostaci sustava. Budući da novca za neovisne revizore i certificiranje po ISO ili nekoj drugoj standardizaciji, nema, odgovorne osobe u bolnicama mogle bi barem načelno uzeti u ruke sigurnosne kontrole predviđene pojedinim standardima i nastojati ih, koliko je to u njihovoj moći, implementirati unutar zdravstvene ustanove. Nije nužno potreban certifikat kao takav da bi bolnice bile sigurne, za početak će biti dovoljno i interno usvojiti dobre prakse koje različiti standardi propisuju, a dostupni su i preko internetskih alata. Sukladno tome, potrebno je napraviti plan implementacije informacijske sigurnosti te, u bolnicama u kojima nedostaje, sastaviti krovni dokument o toj tematici i dopuniti ga s nižim politikama koje preciziraju pojedine aspekte jer ustaljena praksa i nepisana pravila u velikom broju situacija nisu dovoljni i mogu dovesti do još većih problema.

Ono što je realan problem jest nedostatak sluha Ministarstva zdravstva i ostalih državnih tijela za pitanje informacijske sigurnosti. Evidentno je da odgovornost za zabrinjavajuće stanje informacijske sigurnosti u bolnicama snose i ravnatelji. Međutim, s ograničenim proračunskim sredstvima koja dakako da će utrošiti u plaće zaposlenika, lijekove i liječenje pacijenata, ostaje im malo prostora za manevar. Nedopustivo je da bolnice koriste nelicencirane softvere i zastarjele sigurnosne sustave i gube rezervne kopije informacija, a u pojedinim slučajevima, nemaju niti dovoljnu redundantnost za djelovanje u slučaju krize ili katastrofe. To su problemi koje bolnice, ali i institucije u drugim sektorima same za sebe ne mogu riješiti, već im u njima treba strateški partner u vidu države i lokalne te regionalne samouprave.

LITERATURA

Knjige

- Glenny, Misha (2014) *DarkMarket : kako su hakeri postali nova mafija*. Zagreb: Naklada Ljevak.
- Hadjina, Nikola (2009) *Zaštita i sigurnost informacijskih sustava (nastavni materijali sa zbirkom zadataka)*. Zagreb: Fakultet elekrotehnike i računarstva.
- Košutić, Dejan (2012) *9 Steps to Cybersecurity: The Manager's Information Security Strategy Manual*. Zagreb: EPPS Services Ltd.
- Lamza Posavec, Vesna (2006) Metode istraživanja u novinarstvu. Zagreb: Fakultet političkih znanosti.
- Savić, Dean (2015) *Organizirani kriminal: (ne)prepoznata prijetnja.* Zagreb: Jesenski turk.
- Singer, Peter Warren i Friedman, Allan (2014) *Cybersecurity and Cyberwar: what everyone needs to know*. New York: Oxford University Press.

Zbornici

- Brnetić, Damir i dr (2013) Kaznenopravno-forenzička zaštita kritične nacionalne infrastrukture od informatičkih (cyber) ugroza. U: Antoliš, Krunoslav (ur) *Nove sigurnosne ugroze i kritična nacionalna infrastruktura* (str. 34-45). Zagreb: Ministarstvo unutarnjih poslova, Policijska akademija.
- Klaić, Aleksandar i Perešin, Anita (2011) Koncept regulativnog okvira informacijske sigurnosti. U: Toth, Ivan (ur) *Dani kriznog upravljanja* (str. 678-708). Velika Gorica: Veleučilište Velika Gorica.
- Knapp, Kenneth J. i Boulton, Willieam R. (2009) Ten Information Warfare Trends. U: Janczewski, Lech J. i Colarik, Andrew M. (ur) *Cyber Warfare and Cyber Terrorism* (str. 17-25). Hershey: Information Science Reference
- Košutić, Dejan (2009) Primjena normi informacijske sigurnosti na primjeru HEP-a. U: Krajcar, Slavko (ur) *Energetska sigurnost i kritična infrastruktura* (161-171). Zagreb: Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva.

- Košutić, Dejan i Matika Dario (2009) Korporativna i informacijska sigurnost U: Krajcar, Slavko (ur) *Energetska sigurnost i kritična infrastruktura* (171-185). Zagreb: Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva.
- Matika, Dario (2009) Energetska sigurnost i kritična infrastruktura – pregled rezultata istraživanja. U: Matika, Dario i Poljanec-Borić, Saša (ur) *Kritična infrastruktura u Hrvatskoj: Prema novom sustavu sigurnosti i zaštite* (45-59). Zagreb: Institut za istraživanje i razvoj obrambenih sustava MORH-a, Institut društvenih znanosti Ivo Pilar.
- Nađ, Ivan i Adelsberger, Zdenko (2016) Informacijska sigurnost u kontekstu kriznog upravljanja . U: Nađ, Ivan (ur) *Dani kriznog upravljanja* (116-126). Velika Gorica: Veleučilište Velika Gorica.
- Perešin, Anita i Klaić, Aleksandar (2012) Uloga kibernetičke sigurnosti u zaštiti kritične infrastrukture. U: Toth, Ivan (ur) *Dani kriznog upravljanja* (str. 335-357). Velika Gorica: Veleučilište Velika Gorica.
- Slaveski, Stojan i Popovska, Biljana (2015) Cyber prijetnje kao izazov za upravljanje u kriznim uvjetima, s posebnim osvrtom na Republiku Makedoniju. U: Nađ, Ivan (ur) *Dani kriznog upravljanja* (str. 33-63). Velika Gorica: Veleučilište Velika Gorica.

Članci

- Bachmann, Sascha-Dominik i Gunneriusson, Håkan (2015) Hybrid wars: the 21st-centrury's new threats to global peace and security. *Scientia Militaria: South African Journal of Military Studies* 43(1): 77-98.
- Brzica, Nikola (2015) Kolaps 22. rujna bio je upozorenje o ranjivosti RH na kibernetičke napade. *Defender* 1(1): 33-35.
- Dukić, Snježana (2016) Odgovor na cyber prijetnje. *Hrvatski vojnik* 25(504): 33-36.
- Kovačević, Božo (2014) Cyberwar – američka izlika za novi hladni rat? *Polemos: časopis za interdisciplinarna istraživanja rata i mira* 16(32): 91-110.
- Orehovec, Zvonko (2016) 25 godina od osamostaljenja, i dalje bez Strategije nacionalnog razvoja. *Defender* 2(5): 28-31.

Diplomski radovi, završni specijalistički/doktorski i stručni radovi

- Bond, Margaret (2007) *Hybrid War: A New Paradigm for Stability Operations in Failing States*. Strategy Research Project. Carlisle, Pennsylvania: U.S. Army War College.
- Juran, Ana (2014) *Sigurnost informacijskih sustava*. Diplomski rad. Rijeka: Pomorski fakultet u Rijeci.
- Klaić, Aleksandar (2010) Pregled stanja i trendova u suvremenoj politici informacijske sigurnosti i metodama upravljanja informacijskom sigurnošću. *Kvalifikacijski doktorski ispit.* Zagreb: Fakultet elektrotehnike i računarstva. https://www.fer.unizg.hr/_download/repository/KvalifikacijskiDrIspit_AK_08022010.pdf Pristupljeno 15. kolovoza 2016.
- Majić, Dinko (2015) *Kibernetička sigurnost i zaštita kritične infrastrukture*. Završni specijalistički rad. Zagreb: Fakultet političkih znanosti.
- Ugren, Vladimir (2012) *Cyber kriminal*. Završni specijalistički rad. Beograd: Univerzitet Singidunum.
- Vuković, Hrvoje (2012) *Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj*. Završni specijalistički rad. Zagreb: Fakultet političkih znanosti.

Pravni akti i norme

- Hrvatski sabor (2002) Strategija nacionalne sigurnosti Republike Hrvatske. *Narodne novine* 32.
- Hrvatski sabor (2007) Zakon o informacijskoj sigurnosti. *Narodne novine* 79.
- Hrvatski sabor (2013) Zakon o kritičnim infrastrukturama. *Narodne novine* 56.
- Hrvatski sabor (2014) Zakon o državnoj informacijskoj infrastrukturi. *Narodne novine* 92.
- Hrvatski sabor (2017) Strategija nacionalne sigurnosti Republike Hrvatske. *Narodne novine* 73.
- Vlada Republike Hrvatske (2005) Nacionalni program informacijske sigurnosti u Republici Hrvatskoj.

- Vlada Republike Hrvatske (2015) Odluka o donošenju Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti. Narodne novine 108.
- Vlada Republike Hrvatske (2016) Odluka o osnivanju Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost. *Narodne novine* 61.
- International Organization for Standardization/International Electrotechnical Commission (2013a) *Information technology — Security Techniques — Code of practice for information security controls (ISO/IEC 27002).*
- International Organization for Standardization/International Electrotechnical Commission (2013b) *Information technology — Security techniques — Information security management systems — Requirements (ISO/IEC 27001).*

Ostali internetski izvori

- Antibot.hr (2016a) Hrvatska druga po ransomware napadima. http://www.antibot.hr/blog/2016/11/11/malver/. Pristupljeno 3. siječnja 2017.
- Antibot.hr (2016b) Širenje zlonamjernog koda putem društvenih mreža. http://www.antibot.hr/blog/2016/11/29/malicioz/. Pristupljeno 3. siječnja 2017.
- Antibot.hr (2017) http://www.antibot.hr/about-us/osnovne-informacije.html. Informacije. Pristupljeno 3. siječnja 2017.
- BSA (2015) EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace. http://cybersecurity.bsa.org/. Pristupljeno 30. lipnja 2016.
- Ccdcoe.org (2016) Cyber Security Strategy Documents. https://ccdcoe.org/cyber-security-strategy-documents.html. Pristupljeno 17. kolovoza 2016.
- CERT-EU (2017) WannaCry Ransomware Campaign Exploiting SMB Vulnerability. https://cert.europa.eu/static/SecurityAdvisories/2017/CERT-EU-SA2017-012.pdf. Pristupljeno 28. svibnja 2017.
- Cis.hr (2013) CIS prestaje pratiti provale na hrvatske web poslužitelje. http://www.cis.hr/opcenito/cis-prestaje-pratiti-provale-na-hrvatske-web-posluitelje.html. Pristupljeno 15. srpnja 2016.
- Emm, David i dr (2016) IT threat evolution in Q3 2016. Kaspersky Lab. https://securelist.com/files/2016/11/KL_Q3_Malware_Report_ENG.pdf. Pristupljeno 3. siječnja 2017.

- Halkyn Consulting (2013) ISO27001 compliance checklist available for download. http://www.halkynconsulting.co.uk/a/2013/10/iso27001-compliance-checklist/. Pristupljeno 10. travnja 2017.
- Independent Security Evaluators (2016). Securing Hospitals: A research study and blueprint. https://securityevaluators.com/hospitalhack/. Pristupljeno 10. lipnja 2017.
- Index.hr (2017) Klaićeva nema novca: Sedmero djece neće dobiti lijek koji im može produžiti život. http://www.index.hr/black/clanak/klaiceva-nema-novca-sedmero-djece-nece-dobiti-lijek-koji-im-moze-produziti-zivot/976469.aspx. Pristupljeno 13. lipnja 2017.
- Ipress.rtl.hr (2013) Veliki projekt Vlade: Objedinjavanje optičke infrastrukture, brzi internet za sve. 17. siječnja. http://ipress.rtl.hr/gospodarstvo/veliki-projekt-vlade-objedinjavanje-opticke-infrastrukture-brzi-internet-za-sve-25767.html. Pristupljeno 15. veljače 2017.
- ISO27k Forum (2016) Documenation and records required for ISO/IEC 27001 certifiction. http://www.iso27001security.com/ISO27k_ISMS_Mandatory_documentation_checklist_release_1.docx . Pristupljeno 10. travnja 2017.
- Ivezić, Bernard (2014) U 2014. u cyber-kriminalnim napadima nije bilo oštećenih PBZ klijenata. *Poslovni.hr*. 21. srpnja. http://www.poslovni.hr/tehnologija/u-2014-u-cyber-kriminalnim-napadima-nije-bilo-ostecenih-pbz-klijenata-275871. Pristupljeno 3. siječnja 2017.
- Košutić, Dejan (2017) ISO 27001 gap analysis vs. risk assessment. *Advisera.com*. https://advisera.com/27001academy/knowledgebase/iso-27001-gap-analysis-vs-risk-assessment/. Pristupljeno 10. travnja 2017.
- Latković, Goran (2016) Hakirano ministarstvo, stručnjaci upozoravaju: „Iza ovoga bi mogla biti neka druga država, ovo je tek početak“. *Rtl.hr*. 3. prosinca. http://www.vijesti.rtl.hr/novosti/hrvatska/2022881/hakirano-ministarstvo-strucnjaci-upozoravaju-iza-ovoga-bi-mogla-biti-neka-druga-drzava-ovo-je-tek-pocetak/. Pristupljeno 17. prosinca 2016.
- Laušić, Frenki (2015) Pukla HT-ova mreža: vrijeme je da konačno država izgradi svoju! *Slobodnadalmacija.hr*. 23. rujna. http://www.slobodnadalmacija.hr/novosti/hrvatska/clanak/id/287211/pukla-ht-ova-mreza-vrijeme-je-da-konacno-drzava-izgradi-svoju. Pristupljeno 5. kolovoza 2016.

- Ministarstvo zdravstva – državni proračun za 2017-2019. godine. https://zdravlje.gov.hr/UserDocsImages//2017%20Financijski%20planovi%20i%20strate%C5%A1ki%20dokumenti,%20javna%20nabava//MINISTARSTVO%20ZDRAVSTVA%20%20-%20DR%C5%BDAVNI%20PRORA%C4%8CUN%20ZA%20%202017%20-%202019%20%20GODINE.xlsx. Pristupljeno 10. lipnja 2017
- MTU (Međunarodna telekomunikacijska unija) ITU (2015) Global Cybersecurity Index & Cyberwellness Profiles. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf Pristupljeno 17. veljače 2017.
- NATO (2016) Warshaw Summit Communiqué. www.nato.int/cps/en/natohq/official_texts_133169.htm. Pristupljeno 9. veljače 2017.
- NCERT (2017a) Izvješće o aktivnostima Nacionalnog Cert-a: Pregled sigurnosti na Internetu u RH i u svijetu u 2016. godini. http://www.cert.hr/sites/default/files/NCERT-izvjes%CC%8Ctaj-2016.pdf. Pristupljeno 28. svibnja 2017.
- NCERT (2017b) O nacionalnom CERT-u. http://www.cert.hr/onama. Pristupljeno 28.svibnja 2017.
- Passeri, Paolo (2016) May 2016 Cyber Attacks Statistics. *Hackmaggedon.com*. 19. lipnja. http://www.hackmageddon.com/2016/06/19/may-2016-cyber-attacks-statistics/. Pristupljeno 4. siječnja 2017.
- Tofan, Dan; Nikolakopoulos, Theodoros; Darra, Eleni (2016) The cost of incidents affecting CIIs. *Enisa.* https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis Pristupljeno 17. kolovoza 2016.
- Tomić, Dražen (2014) [NAPOKON]: Objedinjena optička infrastruktura državnih firmi. ICTbusiness.info. 21 veljače. http://www.ictbusiness.info/telekomunikacije/napokon-objedinjena-opticka-infrastruktura-drzavnih-firmi. Pristupljeno 15. veljače 2017.
- University of Cambridge – Institute for Manufacturing. (2017) Gap analysis. http://www.ifm.eng.cam.ac.uk/research/dstools/gap-analysis/. Pristupljeno 12. veljače 2017.
- UVNS (Ured Vijeća za nacionalnu sigurnost) (2017) Informacijska sigurnost. http://www.uvns.hr/hr/normativni-akti/informacijska-sigurnost Pristupljeno 15. veljače 2017.

- Van der Meulen, Nicole; Eun A Jo; Soesanto Stefan (2015) Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses. *European Parliament.* http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf. Pristupljeno 5. kolovoza 2016.
- WikiLeaks (2015) Hacking Team. https://wikileaks.org/hackingteam/emails/?q=&mfrom=.hr&mto=&title=&notitle=&date=&nofrom=&noto=&count=1000&sort=2#searchresult. Pristupljeno 3. siječnja 2017.

PRILOZI

Prilog 1: Anonimizirani popis tvrtki/institucija pozvanih na sudjelovanje u istraživanju

R.BR.	TVRTKA/ INSTITUCIJA	ŽUPANIJA	STATUS	POVRATNA INFORMACIJA
ZDRAVSTVENI SEKTOR				
1	Bolnica 1	Grad Zagreb	Javna	Sudjelovali u istraživanju
2	Bolnica 2	Grad Zagreb	Javna	Sudjelovali u istraživanju
3	Bolnica 3	Krapinsko-zagorska	Javna	Sudjelovali u istraživanju
4	Bolnica 4	Grad Zagreb	Javna	Nije odgovoreno
5	Bolnica 5	Grad Zagreb	Javna	Nije odgovoreno
6	Bolnica 6	Grad Zagreb	Javna	Iskazali interes, ali na kraju odustali
7	Bolnica 7	Grad Zagreb	Javna	Nakon uzastopnih napora odgovorili, ali nisu bili zainteresirani te na kraju nisu pristali
8	Bolnica 8	Grad Zagreb	Privatna	Nije odgovoreno
9	Bolnica 9	Grad Zagreb	Privatna	Nije odgovoreno
10	Bolnica 10	Grad Zagreb	Privatna	Nije odgovoreno
11	Bolnica 11	Grad Zagreb	Privatna	Iskazali interes, ali odustali
12	Bolnica 12	Varaždinska županija	Javna	Nije odgovoreno
13	Bolnica 13	Sisačko-moslavačka županija	Javna	Nije odgovoreno
14	Bolnica 14	Koprivničko-križevačka	Javna	Nije odgovoreno
15	Bolnica 15	Virovitičko-podravska	Javna	Nije odgovoreno
16	Bolnica 16	Bjelovarsko-bilogorska županija	Javna	Nije odgovoreno
17	Bolnica 17	Međimurska	Javna	Iskazali interes, ali odustali
18	Bolnica 18	Grad Zagreb	Privatna	Iskazali interes, ali odustali
19	Bolnica 19	Karlovačka	Javna	Odbili sudjelovati u

		županija		istraživanju
ENERGETSKI SEKTOR				
20	Energetska tvrtka1	Grad Zagreb		Sudjelovali u istraživanju
21	Energetska tvrtka1	Grad Zagreb	Privatna s državnim udjelom	Sudjelovali u istraživanju
22	Energetska tvrtka1	Grad Zagreb	Državna	Nije odgovoreno
23	Energetska tvrtka1	Grad Zagreb	Privatna	Nije odgovoreno
IT SEKTOR				
24	IT tvrtka 1	Grad Zagreb	Privatna	Nije odgovoreno
25	IT tvrtka 2	Grad Zagreb	Privatna	Nije odgovoreno
26	IT tvrtka 3	Grad Zagreb	Privatna	Nije odgovoreno

Prilog 2: Ukupni rezultati GAP analize u zdravstvenim ustanovama

REF.	USKLAĐENOST MJERA ZAŠTITE S ISO/IEC 27001:2013		REZULTATI USKLAĐENOSTI U POSTOTCIMA		
ID	**KONTROLA PO ANNEXU ISO/IEC 27001:2013 STANDARDA**	**OPIS**	**Bolnica 1**	**Bolnica 2**	**Bolnica 3**
A.5	**SIGURNOSNA POLITIKA**				
A.5.1	**Usmjerenje rukovodstva za sigurnost informacija**		0.00	0.00	62.50
A.5.1.1	Politike informacijske sigurnosti	Rukovodstvo mora definirati i odobrriti skup politika informacijske sigurnosti, objaviti ih i priopćiti zaposlenicima i odgovarajućim vanjskim stranama.	0	0	50
A.5.1.2	Preispitivanje politika informacijske sigurnosti	Politike informacijske moraju se preispitivati u planiranim intervalima ili u slučaju pojava značajnih promjena, kako bi se osigurala njihova pogodnost, adekvatnost i efektivnost.	0	0	75
PROSJEČNA VRIJEDNOST PODRUČJA:			0.00	0.00	62.50
A.6	**ORGANIZACIJA INFORMACIJSKE SIGURNOSTI**				
A.6.1	**Unutarnja organizacija**		65.00	60.00	65.00
A.6.1.1	Odgovornosti i uloge za sigurnost informacija	Sve uloge i odgovornosti vezane uz informacijsku sigurnost moraju biti definirane i dodijeljene.	50	75	75

A.6.1.2	Razdvajanje dužnosti	Da bi se smanjile prilike za neovlaštenu ili nenamjernu modifikaciju ili zloupotrebu imovine tvrtke, moraju se razdvojiti konfliktne dužnosti i područja odgovornosti.	75	75	75
A.6.1.3	Kontakti s ovlaštenim tijelima	Moraju se održavati odgovarajući kontakti s nadležnim i ovlaštenim tijelima.	75	25	100
A.6.1.4	Kontakti sa specijalnim interesnim grupama	Moraju se održavati odgovarajući kontakti sa specijaliziranim grupama i profesionalnim udruženjima i forumima iz domene informacijske sigurnosti.	75	100	50
A.6.1.5	Sigurnost informacija u upravljanju projektima	Sigurnost informacija mora se uzeti u obzir u upravljanju projektima, neovisno o vrsti projekta.	50	25	25
A.6.2	**Prijenosni/mobilni uređaji i rad s udaljenosti**		25.00	25.00	62.50
A.6.2.1	Politika mobilnih uređaja	Politike i pomoćne mjere sigurnosti moraju biti usvojene na adekvatan način kako bi se upravljalo rizicima nastalim korištenjem prijenosnih/mobilnih uređaja.	25	50	50
A.6.2.2	Rad s udaljenosti	Moraju biti implementirane politika i pomoćne mjere sigurnosti prilikom rada s udaljenosti, a da bi se zaštitile informacije kojima se pristupa, koje se obrađuju i čuvaju na udaljenim lokacijama.	25	0	75
PROSJEČNA VRIJEDNOST PODRUČJA:			53.57	50.00	64.29
A.7	**SIGURNOST VEZANA UZ OSOBLJE**				
A.7.1	**Prije zapošljavanja**		62.50		37.50
A.7.1.1	Provjera kandidata	Moraju se provesti zasebne provjere zbog verifikacije svih kandidata za zaposlenje, u skladu s odgovarajućim zakonima, propisima i etičkim pravilima, a razmjerno poslovnim zahtjevima, stupnju klasifikacije informacija koje radno mjesto zahtjeva i sagledanim rizicima.	75		50

A.7.1.2	Uvjeti zapošljavanja	U ugovoru o radu ili drugim oblicima sporazumne suradnje sa zaposlenicima i suradnicima moraju biti definirane njihove obveze i odgovornosti u pogledu informacijske sigurnosti.	50		25
A.7.2	**Tijekom rada/radnog odnosa**		16.67		33.33
A.7.2.1	Odgovornosti rukovodstva	Rukovodstvo tvrtke mora zahtjevati od svih zaposlenih i suradnika primjenu informacijske sigurnosti u skladu s uspostavljenom politikom i procedurama u tvrtki.	0		25
A.7.2.2	Upoznavanje s informacijskom sigurnošću, obrazovanje i obuka	Svi zaposleni u tvrtki, i onda kada je to bitno – vanjski suradnici, redovito moraju proći odgovarajuću obuku i obnavljati/nadopunjavati znanja o politici i procedurama u organizaciji, na onaj način koji odgovara njihovoj poslovnoj funkciji.	25		50
A.7.2.3	Disciplinski postupak	Mora postojati službeni i obznanjen disciplinski postupak čija je svrha poduzimanje aktivnosti protiv zaposlenika koji su narušili informacijsku sigurnost.	25		25
A.7.3	**Prekid ili promjena uvjeta zapošljavanja**		75.00		50
A.7.3.1	Odgovornosti prilikom prestanka zaposlenja	Odgovornosti i dužnosti koje se odnose na zaštitu informacija, a koje ostaju važeće i nakon prestanka ili promjene uvjeta zapošljavanja moraju biti definirane te jasno iskomunicirane i priopćene zaposlenicima, sadržane u ugovoru te se primjenjivati.	75		50
PROSJEČNA VRIJEDNOST PODRUČJA:			41.67		37.50
A.8	**UPRAVLJANJE RESURSIMA/IMOVINOM**				
A.8.1	**Odgovornost za resurse/imovinu**		50.00	37.50	43.75

A.8.1.1	Popisivanje imovine	Imovina i resursi povezani s informacijama i opremom za obradu informacija moraju biti identificirani i popisani, a popis se mora redovito održavati i revidirati.	50	50	50
A.8.1.2	Vlasništvo nad imovinom	Popisana imovina mora imati definirane vlasnike.	75	25	50
A.8.1.3	Prihvatljivo korištenje imovine	se identificirati, dokumentirati i implementirati pravila za prihvatljivo korištenje informacija i resursa povezanih s informacijama i opremom za obradu informacija.	25	50	50
A.8.1.4	Vraćanje imovine	Svi zaposlenici i vanjski suradnici moraju vratiti svu imovinu i organizacijske resurse koje posjeduju nakon prestanka njihovog zaposlenja, ugovora ili sporazuma.	50	25	25
A.8.2	**Klasificiranje informacija**		16.67	41.67	25.00
A.8.2.1	Klasifikacija informacija	Informacije se moraju klasificirati sukladno zakonskim zahtjevima, njihovoj vrijednosti, kritičnosti i osjetljivosti na neovlašteno korištenje/otkrivanje i/li modifikaciju.	0	75	25
A.8.2.2	Označavanje informacija	Za označavanje informacija mora se razviti i implementirati odgovarajući skup procedura, u skladu sa shemom klasificiranja koji je tvrtka usvojila.	0	0	0
A.8.2.3	Postupanje s imovinom	Za postupanje s imovinom moraju se razviti i implementirati procedure u skladu sa shemom klasificiranja koji je tvrtka usvojila.	50	50	50
A.8.3	**Postupanje s medijima za pohranu**		41.67	41.67	50.00
A.8.3.1	Upravljanje prijenosnim medijima/uređajima	Moraju se implementirati procedure za menadžment/upravljanje prijenosnim medijima za pohranu u skladu sa shemom klasificiranja podataka koju je tvrtka usvojila.	25	50	50

A.8.3.2	Rashodovanje prijenosnih medija	Kada više nisu potrebni, mediji za pohranu podataka moraju se rashodovati na siguran način primjenom formalnih procedura.	75	50	75
A.8.3.3	Fizički prijenos medija	Mediji za pohranu koji sadrže informacije moraju biti zaštićeni od neovlaštenog pristupa, zlouporabe ili oštećenja prilikom transporta.	25	25	25
PROSJEČNA VRIJEDNOST PODRUČJA:			37.50	40.00	40.00
A.11	**FIZIČKA SIGURNOST I SIGURNOST U OKRUŽENJU**				
A.11.1	**Sigurnosna područja**		70.83	83.33	66.67
A.11.1.1	Zona razdvajanja fizičke sigurnosti	Da bi se zaštitila područja u kojima se nalaze osjetljive ili kritične informacije i oprema za obradu informacija, moraju se definirati sigurnosne zone razdvajanja.	75	100	75
A.11.1.2	Kontrole fizičkog ulaska	Sigurnosna područja moraju biti zaštićena kontrolama ulaza kako bi se osigurao pristup samo ovlaštenom osoblju.	75	75	75
A.11.1.3	Zaštita ureda, prostorija i sredstava	Treba projektirati i primijeniti fizičku sigurnost ureda, prostorija i sredstava.	75	75	50
A.11.1.4	Zaštita od vanjskih prijetnji i prijetnji iz okruženja	Mora se projektirati i primijeniti fizička zaštita od prirodnih katastrofa, zlonamjernih upada ili nesreća.	100	75	100
A.11.1.5	Rad u sigurnosnim zonama	Moraju se projektirati i primijeniti pravila za rad u sigurnim područjima.	50	100	25
A.11.1.6	Područja javnog pristupa, isporuke i utovara	Pristupne točke, kao što su područja za isporuku i utovar, kao i druga mjesta na kojima neovlašteni ljudi mogu ući u službene prostorije, moraju se kontrolirati i, ako je to moguće, izdvojiti od opreme za obradu informacija kako bi se izbjegao neovlašten pristup.	50	75	75
A.11.2	**Zaštita opreme**		69.44	69.44	77.78

A.11.2.1	Postavljanje i zaštita opreme	Oprema se mora postaviti ili zaštititi tako da se smanje rizici od prijetnji i opasnosti okruženja ili neovlašten pristup.	50	50	50
A.11.2.2	Pomoćne funcije za podršku	Oprema mora biti zaštićena od nestanka struje i drugih prekida zbog otkazivanja pomoćnih funkcija za podršku.	100	100	100
A.11.2.3	Sigurnost postavljanja kablova	Kablovi za napajanje i telekomunikacije moraju biti zaštićeni od prisluškivanja, ometanja ili oštećenja.	100	100	100
A.11.2.4	Održavanje opreme	Oprema se mora ispravno održavati kako bi se osigurala raspoloživost i integritet.	50	100	100
A.11.2.5	Premještanje/iznošenje opreme	Oprema, informacije ili softver ne smiju se premještati bez dozvole.	75	75	75
A.11.2.6	Sigurnost opreme i imovine iznošene van tvrtke	Sigurnosni mehanizmi moraju se primjenjivati na premještenu opremu zbog rizika rada izvan prostorija organizacije.	50	50	75
A.11.2.7	Sigurno rashodovanje ili ponovno korištenje opreme	Svi dijelovi opreme koji sadrže prostor za čuvanje podataka moraju biti verificirani kako bi se osiguralo da su svi osjetljivi podaci i licencirani softveri prije otpisa ili ponovnog korištenja uklonjeni ili sigurno precrtani.	50	75	75
A.11.2.8	Nenadgledana korisnička oprema	Korisnici moraju osigurati da je opremu bez nadzora adekvatno zaštićena.	100	50	75
A.11.2.9	Politika praznog stola i praznog ekrana	Za pokretne medije za skladištenje i papire mora se usvojiti politika praznog stola te za sredstva za obradu informacija – politika praznog ekrana.	50	25	50
PROSJEČNA VRIJEDNOST PODRUČJA:			70.00	75.00	73.33
A.12	**OPERATIVNA SIGURNOST/SIGURNOST RADNIH OPERACIJA**				
A.12.1	**Radne procedure i odgovornosti**		81.25	75.00	81.25

A.12.1.1	Dokumentirane radne procedure	Radne procedure moraju biti dokumentirane i dostupne svim korisnicima koji ih trebaju.	50	75	50
A.12.1.2	Upravljanje promjenama	Moraju se kontrolirati promjene u organizaciji, poslovnim procesima, oprema za obradu podataka i na sustavima koje utječu na sigurnost podataka.	75	75	100
A.12.1.3	Upravljanje prostorom	Korištenje resursa mora se nadgledati, podešavati i raditi izračuni za potrebnim kapacitetima u budućnosti kako bi se osigurali potrebne performanse sistema.	100	75	75
A.12.1.4	Razdvajanje okruženja za razvoj, ispitivanje i rad	Prostor za razvoj, ispitivanje i rad moraju biti međusobno razdvojeni kako bi se smanjili rizici od neovlaštenog pristupa ili promjena u radnim uvjetima.	100	75	100
A.12.2	**Zaštita od zlonamjernog softvera**		75.00	50.00	50.00
A.12.2.1	Kontrole protiv zlonamjernog softvera	Moraju se implementirati kontrole otkrivanja, sprečavanja i oporavka sistema zaštite od zlonamjernog softvera, u kombinaciji s razvijanjem svijesti korisnika o tome.	75	50	50
A.12.3	**Rezervne (sigurnosne) kopije**		100.00	100.00	25.00
A.12.3.1	Rezervne kopije informacija	Rezervne kopije informacija, softvera i duplikate sistema moraju se redovito izrađivati i ispitivati u skladu s dogovorenim pravilima izrade kopija.	100	100	25
A.12.4	**Zapisivanje i praćenje**		87.50	81.25	81.25
A.12.4.1	Zapisivanje logova o događajima	Moraju se izrađivati zapisi (logovi) o zbivanjima u koje se bilježe aktivnosti korisnika, izuzeci i greške vezane uz sigurnost informacija koje se moraju čuvati i redovno preispitivati.	75	75	75
A.12.4.2	Zaštita informacija u zapisima	Sredstva za logove i informacije u njima moraju biti zaštićene od neovlaštenog mijenjanja i pristupa.	75	75	75
A.12.4.3	Zapisi administratora i operatera	Aktivnosti administratora i sistemskog operatera moraju se zapisivati u logovima koji se štite i preispituju.	100	75	75

A.12.4.4	Sinkronizacija satova	Satovi svih sistema za obradu informacija u organizaciji moraju biti sinkronizirani s nekim dogovorenim izvorom točnog vremena.	100	100	100
A.12.5	**Kontrola operativnog sofvera**		75.00	75.00	75.00
A.12.5.1	Instalacija softvera na operativnim sustavima	Moraju se implementirati procedure za kontrolu instalacije softvera na računalima.	75	75	75
A.12.6	**Upravljanje tehničkim ranjivostima**		75.00	87.50	75.00
A.12.6.1	Kontrola tehničkih ranjivosti	Pravovremeno se moraju prikupljati informacije o tehničkim ranjivostima informacijskih sistema koji se koriste, procjenjivati se izloženost organizacije tim ranjivostima i poduzimati odgovarajuće mjere zbog mogućih rizika.	75	75	75
A.12.6.2	Ograničenja u pogledu instalacije softvera	Pravila koja reguliraju instalaciju softvera od strane korisnika moraju biti uspostavljena i implementirana.	75	100	75
A.12.7	**Održavanje informacijskih sustava**		75.00	75.00	100.00
A.12.7.1	Kontrole za provjeru informacijskih sustava	Zahtjevi za provjeru i radovi koji obuhvaćaju održavanje operativnih sustava moraju se pažljivo planirati i dogovarati kako bi se smanjio rizik od ometanja poslovnih procesa.	75	75	100
PROSJEČNA VRIJEDNOST PODRUČJA:			82.14	78.57	75.00
A.13	**SIGURNOST KOMUNIKACIJA**				
A.13.1	**Upravljanje sigurnošću mreža**		91.67	75.00	91.67
A.13.1.1	Kontrole u mrežama	Mrežama se mora adekvatno upravljati i kontrolirati ih kako bi se zaštitile informacije u sistemima i aplikacijama.	100	100	100
A.13.1.2	Sigurnost mrežnih usluga	U sporazumu o mrežnim uslugama, za sve mrežne usluge moraju biti identificirani i uključeni mehanizmi sigurnosti, razine usluga i zahtjeva za upravljanje, bilo da se one pružaju unutar tvrtke ili se „outsourcaju“.	75	75	75

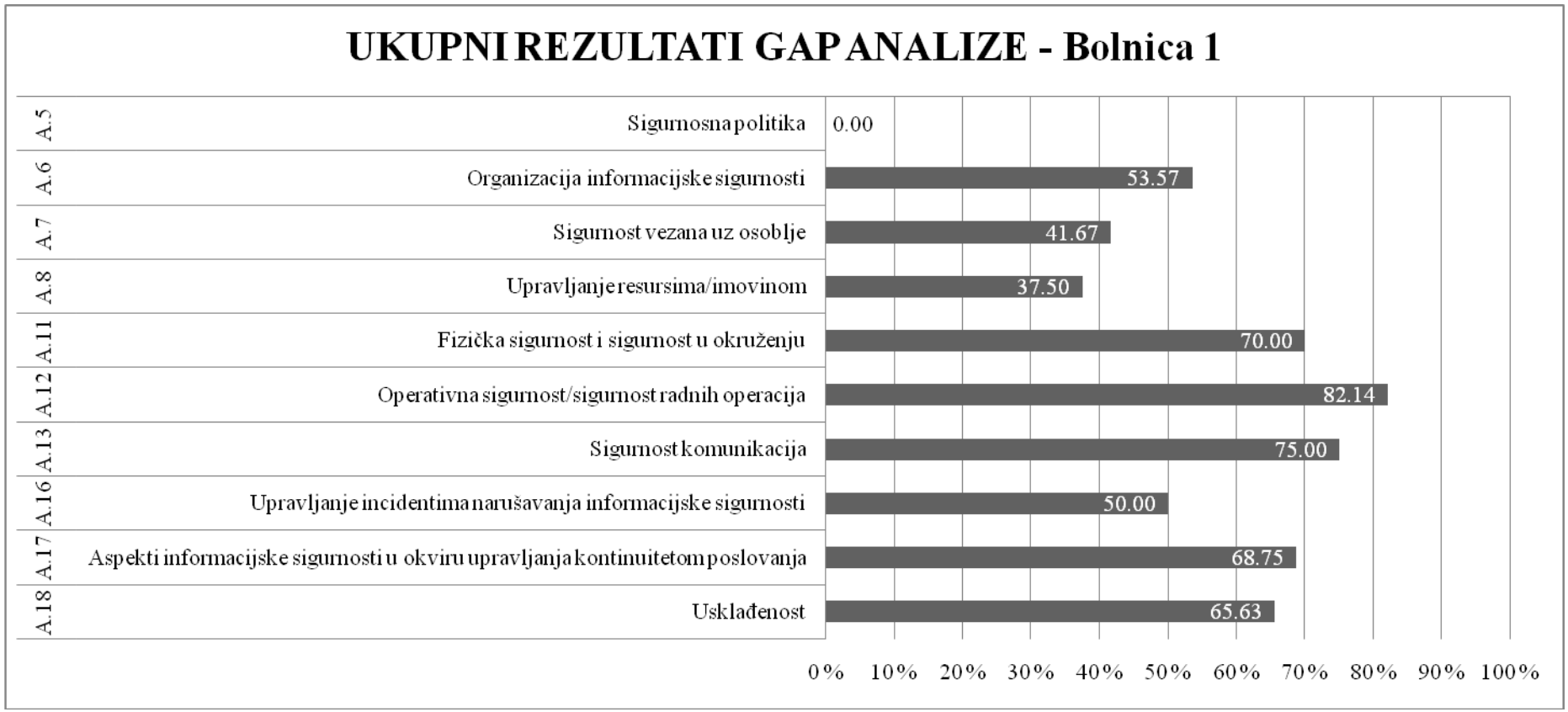
A.13.1.3	Razdvajanje u mreži	U mrežama moraju biti razdvojene grupe informacijskih usluga, korisnici i informacijski sistemi.	100	50	100
A.13.2	**Prijenos informacija**		62.50	68.75	56.25
A.13.2.1	Politike i procedure prilikom prijenosa informacija	Da bi se zaštitio prijenos informacija putem korištenja svih tipova komunikacijskih sredstava, moraju se uspostaviti adekvatne politike, procedure i kontrole.	50	75	50
A.13.2.2	Sporazumi o prijenosu informacija	Sporazumi o prijenosu informaciju moraju obuhvatiti siguran prijenos poslovnih informacija između organizacije i drugih strana.	50	75	50
A.13.2.3	Razmjena elektronskih poruka	Informacije u elektronskoj pošti moraju biti adekvatno zaštićene.	75	50	50
A.13.2.4	Sporazumi o povjerljivosti ili neotkrivanju	o povjerljivosti ili neotkrivanju informacija koji se odnose na tvrtku moraju se redovno preispitivati, dokumentirati i identificirati.	75	75	75
PROSJEČNA VRIJEDNOST PODRUČJA:			75.00	71.43	71.43
A.16	**UPRAVLJANJE INCIDENTIMA NARUŠAVANJA INFORMACIJSKE SIGURNOSTI**				
A.16.1	**Upravljanje incidentima narušavanja informacijske sigurnosti i poboljšavanja**		50.00	53.57	60.71
A.16.1.1	Odgovornosti i procedure	Moraju se uspostaviti odgovornosti rukovodstva i procedure da bi se osigurala brza, efektivna i efikasna reakcija na incidente narušavanja informacijske sigurnosti.	25	50	50
A.16.1.2	Izvještavanje o događajima u vezi s informacijskom sigurnošću	O događajima u vezi s (narušavanjem) informacijske sigurnosti mora se izvještavati se što je brže moguće, preko odgovarajućih linija rukovođenja.	75	75	50

A.16.1.3	Izvještavanje o sigurnosnim slabostima	Od zaposlenika i suradnika koji koriste informacijske sustave mora se zahtjevati da zapisuju i izvještavaju o svakom uočenom ili sumnjivom slabljenju sigurnosti u sustavima ili uslugama vezanim uz informacijsku sigurnost.	75	75	75
A.16.1.4	Ocjenjivanje i odluke o događajima u vezi s informacijskom sigurnošću	Događaji vezani uz informacijsku sigurnost moraju se (pr)ocjenjivati se te se na temelju toga mora odlučiti je li potrebno da se klasificiraju kao incidenti narušavanja informacijske sigurnosti.	50	25	50
A.16.1.5	Odgovor na incidente narušavanja informacijske sigurnosti	Na incidente vezane uz narušavanje informacijske sigurnosti mora se odgovoriti u skladu s dokumentiranim procedurama.	50	50	50
A.16.1.6	Prikupljanje znanja iz incidenata narušavanja informacijske sigurnosti	Prikupljeno znanje iz analiziranja i rješavanja incidenata narušavanja informacijske sigurnosti mora se iskoristiti kao iskustvo za buduće situacije, kako bi se smanjila vjerojatnost ili utjecaj budućih incidenata.	50	50	75
A.16.1.7	Prikupljanje dokaza	Tvrtka mora definirati i primjenjivati procedure za identifikaciju, prikupljanje, nabavku i čuvanje informacija koje mogu služiti kao dokaz.	25	50	75
PROSJEČNA VRIJEDNOST PODRUČJA:			50.00	53.57	60.71
A.17	**ASPEKTI INFORMACIJSKE SIGURNOSTI U OKVIRU UPRAVLJANJA KONTINUITETOM POSLOVANJA**				
A.17.1	**Kontinuitet informacijske sigurnosti**		58.33	58.33	50.00
A.17.1.1	Planiranje kontinuiteta informacijske sigurnosti	Tvrtka mora odrediti svoje zahtjeve koji se odnose na informacijsku sigurnost i kontinuitet upravljanja informacijskom sigurnošću u nepovoljnim situacijama, kao što su krize i/li katastrofe.	75	50	25

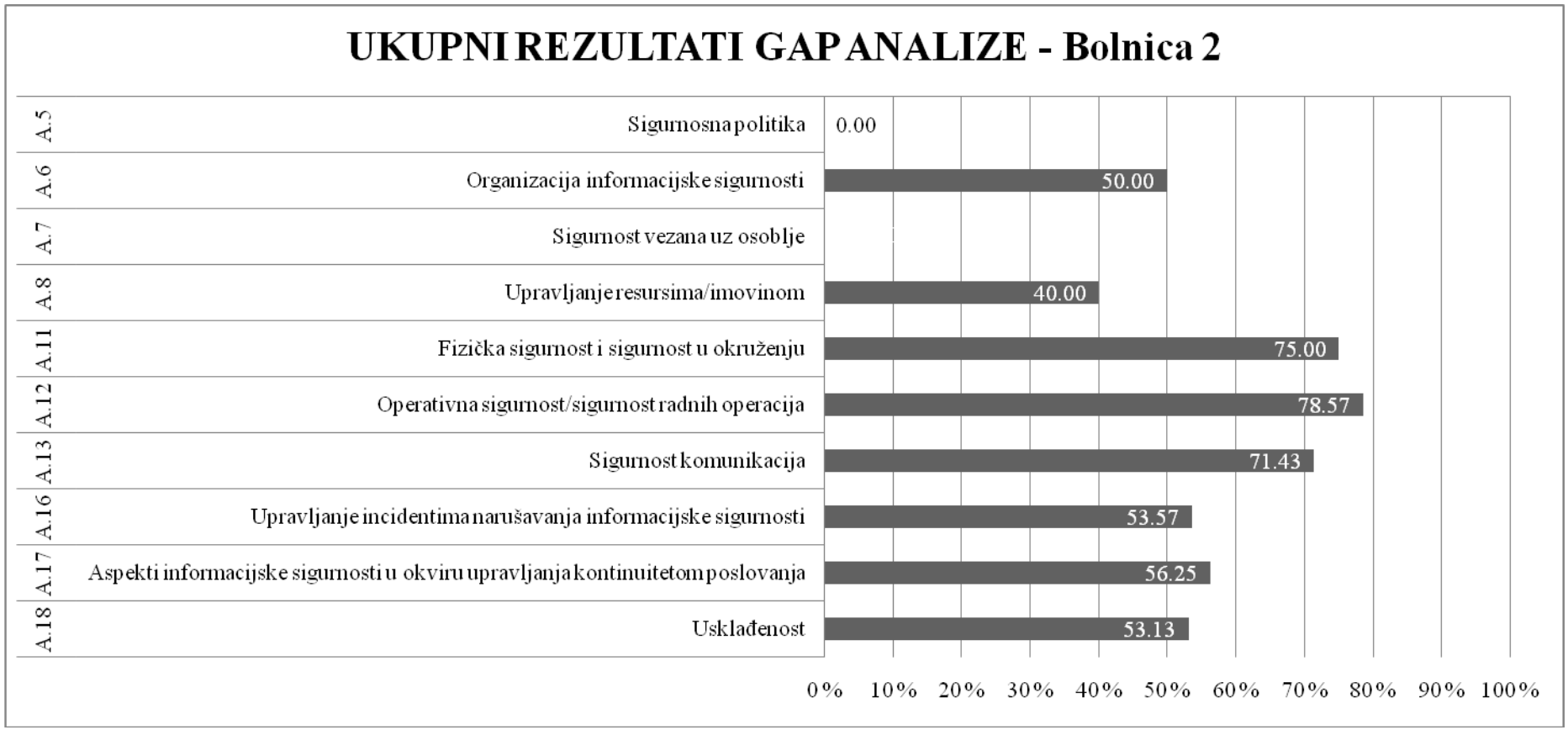
A.17.1.2	Implementacija kontinuiteta informacijske sigurnosti	Tvrtka mora uspostaviti, dokumentirati, implementirati te održavati procese, procedure i kontrole da bi se osigurala zahtjevana razina kontinuiteta za sigurnost informacija tijekom nepovoljnih situacija.	25	50	50
A.17.1.3	Verifikacija, preispitivanje i procjenjivanje kontinuiteta informacijske sigurnosti	Tvrtka mora verificirati/provjeravati uspostavljene i implementirane kontrole kontinuiteta informacijske sigurnosti u redovnim intervalima da bi se osiguralo da su te kontrole važeće i efektivne tijekom nepovoljnih situacija.	75	75	75
A.17.2	**Redundancija**		100.00	50.00	25.00
A.17.2.1	Dostupnost sredstava za obradu informacija	Sredstva za obradu informacija moraju se implementirati s redundancijom koja je dovoljna za zadovoljavanje zahtjeva koji se odnose na dostupnost.	100	50	25
PROSJEČNA VRIJEDNOST PODRUČJA:			68.75	56.25	43.75
A.18	**USKLAĐENOST**				
A.18.1	**Usklađenost sa zakonskim i ugovornim zahtjevima**		80.00	60.00	80.00
A.18.1.1	Identifikacija primjenjivih zakonskih i ugovornih zahtjeva	Tvrtka mora eksplicitno i jasno identificirati, dokumentirati i ažurno održavati sve odgovarajuće zakonske, propisne, statusne i ugovorne zahtjeve vezane uz informacijske sustave i kompaniju u cijelosti.	75	75	75
A.18.1.2	Prava intelektualnog vlasništva	Moraju se implementirati odgovarajuće procedure da bi se osigurala usklađenost s propisima, zakonskim i ugovornim zahtjevima koji se odnose na prava intelektualnog vlasništva i korištenje zaštićenih/autorskih softverskih proizvoda.	75	0	75
A.18.1.3	Zaštita zapisa	Zapisi moraju biti zaštićeni od gubljenja, uništavanja, krivotvorenja, neovlaštenog pristupa i neovlaštenog objavljivanja u skladu s propisima, zakonskim, ugovornim i poslovnim zahtjevima.	100	75	100

A.18.1.4	Tajnost i zaštita osobnih podataka	Mora se osigurati tajnost i zaštita osobnih podataka onako kako se to zahtjeva u odgovarajućim zakonskim aktima i propisima.	50	75	75
A.18.1.5	Propisi za kriptografske kontrole	Kriptografske kontrole moraju se primjenjivati u skladu s odgovarajućim sporazumima, zakonima i propisima.	100	75	75
A.18.2	**Preispitivanja informacijske sigurnosti**		41.67	41.67	50.00
A.18.2.1	Neovisno preispitivanje informacijske sigurnosti	Pristup tvrtke upravljanju informacijskom sigurnošću i njegovoj implementaciji (ciljevima kontrola, kontrolama, politikama, procesima, procedurama za informacijsku sigurnost) mora preispitivati neovisno tijelo u planiranim intervalima ili kada se pojave značajne promjene u tvrtki.	50	50	75
A.18.2.2	Usklađenost s politikama informacijske sigurnosti i standardima	Rukovodstvo redovito mora preispitivati usklađenost informacijskih procesa i procedura u okviru područja svojih odgovornosti s odgovarajućim politikama sigurnosti, standardima i svim drugim sigurnosnim zahtjevima.	25	25	25
A.18.2.3	Preispitivanje tehničke usklađenosti	Redovito se mora preispitivati usklađenost informacijskih sustava s politikama informacijske sigurnosti i odgovarajućim standardima.	50	50	50
PROSJEČNA VRIJEDNOST PODRUČJA:			65.63	53.13	68.75
UKUPNI REZULTATI (UKUPNA USKLAĐENOST):			54.43	47.79	59.73

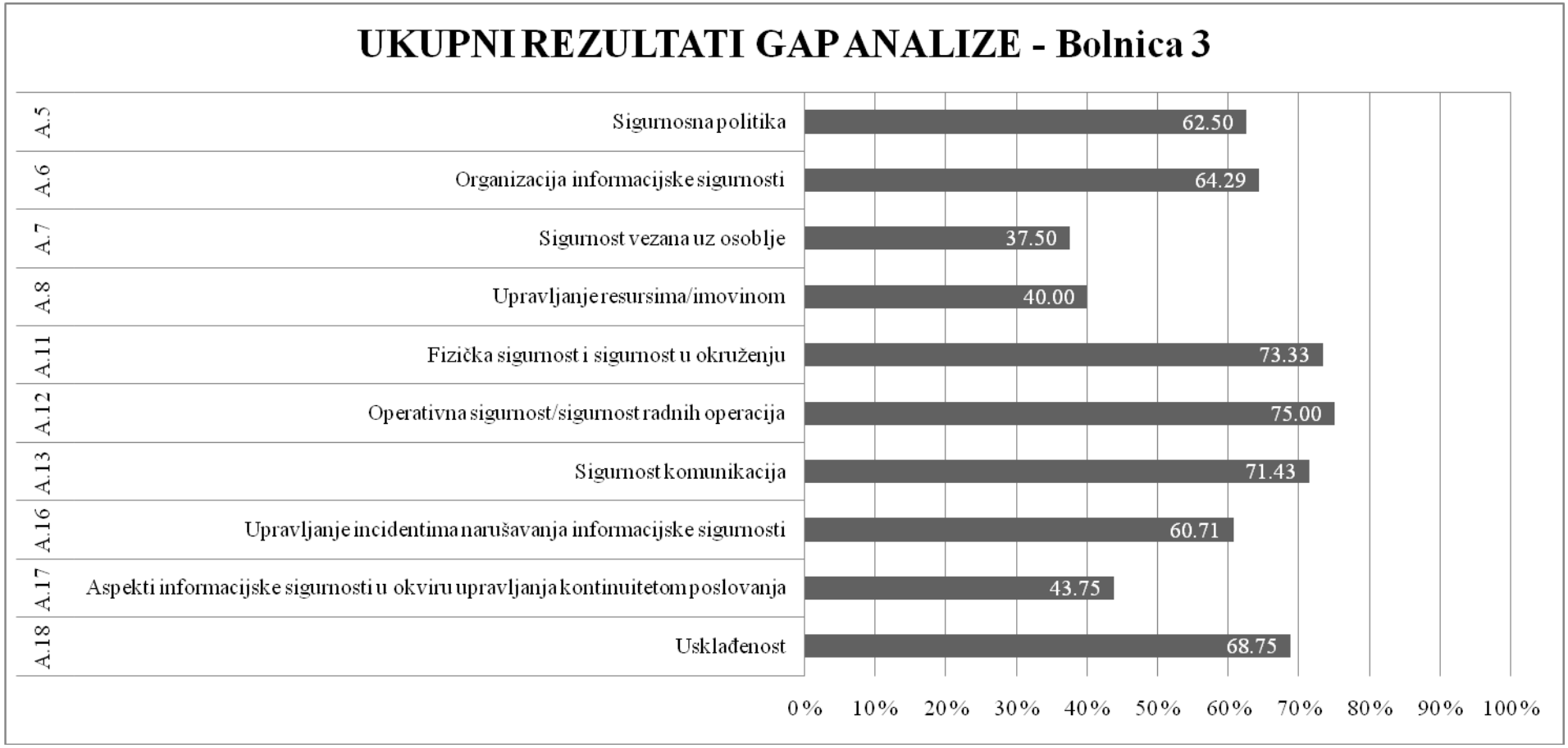
Prilog 3: Grafički prikaz rezultata GAP analize za Bolnicu 1



Prilog 4: Grafički prikaz rezultata GAP analize za Bolnicu 2



Prilog 5: Grafički prikaz rezultata GAP analize za Bolnicu 3



SAŽETAK

Cilj istraživanja bio je utvrditi koje su organizacijske i tehničke slabosti tvrtki iz sektora kritičnih infrastruktura koje bi posredno ili neposredno mogle utjecati na nacionalnu sigurnost Republike Hrvatske. Rad se sastoji od analize regulativnog i institucionalnog okvira vezanog uz tematiku i trenutno stanje na području informacijske i cyber sigurnosti te gap analize (analize rascjepa, jaza) ISO/IEC 27001: 2013 standarda informacijske sigurnosti u tri javno-zdravstvene ustanove i jednoj energetskoj kompaniji. Premda se rezultati zbog ograničenosti uzroka ne mogu generalizirati na kompletni zdravstveni i energetski sustav, narušavanje sigurnosti i jedne bolnice može rezultirati gubljenjem tisuće osobnih podataka i kaosom u cijelom sustavu. Analiza je pokazala da se zbog manjka financijskih sredstava i podkapacitiranosti u analiziranim zdravstvenim institucijama koriste zastarjeli softveri, a osoblje nije dovoljno osviješteno o pitanjima informacijske sigurnosti te ne postoji sistematična politika koja bi na internoj razini regulirala tu tematiku. Za razliku od zdravstvenih ustanova koje u većoj mjeri nisu usklađene sa međunarodno prihvaćenim standardima informacijske sigurnosti, energetska tvrtka u svakodnevnom poslovanju vodi se svim propisanim kontrolama iz ISO standarda.

Ključne riječi: nacionalna sigurnost, informacijska sigurnost, cyber prijetnje, ISO standardi, zdravstvene ustanove, energetske tvrtke, kritična infrastruktura

ABSTRACT

The object of the research was identifying the organizational and technical defficiencies of critical infrastructure companies which could, directly or indirectly,have an effect on the Republic of Croatia's national security.The thesis consists of an analysis of the regulatory and institutional framework related to the subject and the current circumstances in information and cyber security, and an ISO IEC 27001: 2013 gap analysis of information security standards of three state healthcare institutions and one energy company. Although the results cannot be applied to the entire healthcare or energy systems due to a restricted sample, a breach in security of one hospital alone may cause loss of personal data of thousands and result in chaos in the entire system. The analysis has shown that analyzed healthcare institutions use outdated software due to lack of resources and undercapacity, and that the

staff are not sufficiently familiar with information security issues.A systemic policy which would regulate the issue internally is also non-existent.Unlike healthcare institutions, which are largely inconsistent with internationally acclaimed information security standards, the energy company administers all ISO-standard prescribed controls in its day-to-day operations.

Keywords: national security, information security, cyber threats, ISO standards, healthcare institutions, energy companies, critical infrastructure